Special Report
CMU/SEI-97-SR-003

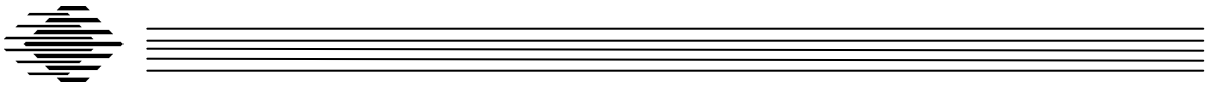
Report to the President's Commission on Critical Infrastructure Protection

James Ellis
David Fisher
Thomas Longstaff
Linda Pesante
Richard Pethia

January 1997

Special Report
CMU/SEI-97-SR-003
January 1997

Report to the President's Commission on Critical Infrastructure Protection



James Ellis

David Fisher

Thomas Longstaff

Linda Pesante

Richard Pethia

CERT[SM] Coordination Center

Unlimited distribution subject to the copyright

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

This report was prepared for the
SEI Joint Program Office
HQ ESC/AXS
5 Eglin Street
Hanscom AFB, MA 01731-2116

The ideas and findings in this report should not be construed as an official DoD position. It is published in the interest of scientific and technical information exchange.
FOR THE COMMANDER

(signature on file)

Thomas R. Miller, Lt Col, USAF
SEI Joint Program Office

This work is sponsored by the U.S. Department of Defense.

Copyright © 1997 by Carnegie Mellon University. This document or excerpts from it may be reproduced and distributed provided credit is given to the CERT Coordination Center and Carnegie Mellon University and provided the material is not used for commercial (for-profit) purposes.

CERT is a service mark of Carnegie Mellon University.

Permission to reproduce this document and to prepare derivative works from this document for internal use is granted, provided the copyright and "No Warranty" statements are included with all reproductions and derivative works.

Requests for permission to reproduce this document or to prepare derivative works of this document for external and commercial use should be addressed to the SEI Licensing Agent.
NO WARRANTY
THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

This work was created in the performance of Federal Government Contract Number F19628-95-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 52.227-7013.

This document is available through Research Access, Inc., 800 Vinial Street, Suite C201, Pittsburgh, PA 15212. Phone: 1-800-685-6510. FAX: (412) 321-2994. RAI also maintains a World Wide Web home page. The URL is http://www.rai.com

Copies of this document are available through the National Technical Information Service (NTIS). For information on ordering, please contact NTIS directly: National Technical Information Service, U.S. Department of Commerce, Springfield, VA 22161. Phone: (703) 487-4600.

This document is also available through the Defense Technical Information Center (DTIC). DTIC provides access to and transfer of scientific and technical information for DoD personnel, DoD contractors and potential contractors, and other U.S. Government agency personnel and their contractors. To obtain a copy, please contact DTIC directly: Defense Technical Information Center / Attn: BRR / 8725 John J. Kingman Road / Suite 0944 / Ft. Belvoir, VA 22060-6218. Phone: (703) 767-8274 or toll-free in the U.S. – 1-800 225-3842).

Use of any trademarks in this report is not intended in any way to infringe on the rights of the trademark holder.

Table of Contents

Executive Summary

The current state of Internet security is cause for concern. Vulnerabilities associated with the Internet put users at risk. Security measures that were appropriate for mainframe computers and small, well-defined networks inside an organization are not effective for the Internet, a complex, dynamic world of interconnected networks with no clear boundaries and no central control. Security issues are not well understood and are rarely given high priority by software developers, vendors, network managers, or consumers.

To compound the problem, the Internet was not originally designed to be secure, and attackers prey on the ongoing lack of security because attacks are so easy and the risk of getting caught is slim. As long as we continue to rank security lower than price, performance, and other features, the growing dependence of the United States on the Internet makes our country vulnerable.

This vulnerability will increase in the future because of the growing ties between the Internet and the critical infrastructures identified in Executive Order 13010. Today, a sustained attack on the Internet can have a serious impact on other critical infrastructures in the United States. In the future, because the ties between critical infrastructures and the Internet will become stronger and more intricate, the impact of an Internet attack could be devastating.

It is essential to take steps now to ensure that the U.S. can resist Internet attacks and that the Internet can continue to perform critical functions in the face of an attack. Although no single approach can ensure Internet security and survivability, a combination of approaches can reduce the risks associated with our ever-increasing dependence on the Internet and the possibility of a sustained attack on it. In this report, we offer recommendations on the role the government can play in reducing risks to the Internet and our other critical infrastructures. These recommendations are summarized below and discussed in detail in Section 5.2.

1. Reporting and Monitoring Threats and Vulnerabilities

a. Designate a single, independent, trusted organization to collect and analyze cybersecurity incident data, and report on quantity, trends, and character of the incidents.

b. Support the establishment of mechanisms for sanitizing and disseminating data on security problems, data that helps the networked community understand the scope and cost of the overall problem.

c. Share threat information available to the government with the private sector to help them accurately gauge the threat they face, especially the international threat.

d. Support the growth and use of global detection mechanisms by using incident response teams to identify new threats and vulnerabilities.

e. Encourage Internet service providers to develop security incident response and other security improvement services for their customers.

2. Education and Security Mechanisms for "Safe Computing"

a. Support the development of educational materials and programs about cyberspace for all users, both children and adults. In particular, support programs that provide early training in security practices and behavior when using the Internet.

b. Invest in awareness campaigns that stress the need for security training for system administrators, network managers, and chief information officers.

c. Facilitate the development and deployment of security mechanisms for information in cyberspace, mechanisms that allow each party to a transaction (or perhaps parents on behalf of their children or companies on behalf of their employees) to decide what precautions and limitations they want.

3. Research and Development

a. Fund research and development in the areas of security and survivability for unbounded systems' architectures with distributed control.

b. Encourage the development of comprehensive toolkits that support network administrators' efforts to operate secure systems; acquisition and operations organizations should drive the market.

c. Support the development of techniques for comprehensive, continuous risk identification and mitigation programs.

4. Use of Standards

a. Establish and encourage acceptance of software security standards as a short-term method to jump-start the process of improving security in Internet products.

b. Create a U.S. government policy that government-purchased computer equipment and software must meet a specified set of security standards; include in this policy a requirement for a security alert service that notifies the customer of vulnerabilities and repairs.

5. Laws and Law Enforcement

a. Support our "cybercops." Allocate appropriate funding to law enforcement agencies to support the training, physical resources, and staff necessary to handle the cybercrimes reported.

b. Ensure that national policy reflects the need of law enforcement to coordinate internationally to solve crimes in cyberspace. Support law enforcement in forming international hot pursuit agreements.

c. Ensure public policy facilitates the widespread use of encryption to protect information and users of cyberspace.

Report to the President's Commission on Critical Infrastructure Protection

Abstract: This report was written for the President's Commission on Critical Infrastructure Protection. Based on the experience of the CERT[SM] Coordination Center, we identify threats to and vulnerabilities of the Internet and estimate the cascade effect that a successful, sustained attack on the Internet would have on the critical national infrastructures set out in Executive Order 13010. Finally, we discuss the implications for public policy and make specific recommendations.

1. Introduction

At this writing, government, commercial, and educational organizations depend on computers to such an extent that day-to-day operations are significantly hindered when the computers are "down." Currently many of the day-to-day operations depend upon connections to the Internet, and new connections are continuously being made to the Internet. In July 1996, an estimated 12,900,000 computers worldwide were connected to the Internet, compared with 130,000 in 1989 and 1,000,000 in 1992—just four years ago.[1] In the future, government, commerce, schools, and individuals are likely to be as dependent on the Internet as they are on telephone, fax, and desktop computers today. Accordingly, Internet security and survivability will become increasingly critical to the stability and well-being of the nation.

Use of the Internet enhances the ability of organizations to conduct their activities in a cost-effective and efficient way. However, along with increased capability and dependence comes increased vulnerability. It is easy to exploit the many security holes in the Internet and in the software commonly used in conjunction with it; and it is easy to disguise or hide the true origin and identity of the people doing the exploiting. Moreover, the Internet is easily accessible to anyone with a computer and a network connection. Individuals and organizations worldwide can reach any point on the network without regard to national or geographic boundaries.

Computers have become such an integral part of American business and government that computer-related risks cannot be separated from general business, health, and privacy risks. Valuable government and business assets are now at risk over the Internet. For example, customer and personnel information may be exposed to intruders. Financial data, intellectual property, and strategic plans may be at risk. The widespread use of databases

[1] This data was obtained from Network Wizards and is available on the Internet at http://www.nw.com/.

leaves the privacy of individuals at risk. Increased use of computers in safety-critical applications, including the storage and processing of medical records data, increases the chance that accidents or attacks on computer systems can cost people their lives.

Techniques that have worked in the past for securing systems will not be effective in the world of unbounded networks, mobile computing, distributed applications, and dynamic computing that we are beginning to see. In the past, use of the Internet was closely linked to telecommunications, with most Internet access achieved through dial-in ports. Today, that link is less significant; there is rapid movement toward increased use of interconnected networks for a broad range of activities, including commerce, education, entertainment, operation of government, and supporting the delivery of health and other human services. Although this trend promises many benefits, it also poses many risks. In short, interconnections are rapidly increasing, and dial-in access isn't required to exploit vulnerabilities in systems, compromise information, or launch denial-of-service attacks.

There are ways to address the problem of Internet security and survivability. Although no single approach is sufficient, a combination of approaches can reduce the risks associated with our ever-increasing dependence on the Internet and the possibility of a sustained attack on it.

In this report, we refer to both the *information infrastructure* and the *Internet.* The information infrastructure is the total collection of digital technology, protocols (rules and conventions), and information on which business, commerce, government, and individuals depend. It includes the "cyber" component of the other critical national infrastructures; but it is also an infrastructure in its own right, with unique characteristics and vulnerabilities. The Internet is the collection of loosely connected networks worldwide that are accessible by individual host computers through a variety of gateways, routers, dial-up connections, Internet access providers, and Internet service providers. The Internet is both an underlying technology and an integral part of the information infrastructure.

In the next section, we describe key factors that contribute to the current state of Internet security. Section 3 provides an assessment of Internet vulnerabilities, along with reasons the Internet is attractive to attackers. In Section 4 we give examples of several ways in which critical national infrastructures depend on the Internet now and will depend on it in the future, and predict the impact a sustained attack on the Internet would have on those infrastructures. Finally, in Section 5 we offer recommendations for improving the security and survivability of the Internet, thus improving the nation's ability to protect its critical infrastructures.

2. Key Factors in the Current State of Internet Security

The current state of Internet security is the result of many factors. In this section, we discuss the key contributing factors. A change in any one of these can change the level of Internet security and survivability.

- Because of the dramatically lower cost of communication on the Internet, use of the Internet is replacing other forms of electronic communication. The Internet itself is growing at an amazing rate, as noted in the introduction.
- There is a continuing movement to distributed, client-server, and heterogeneous configurations. As the technology is being distributed, the management of the technology is often distributed as well. In these cases, system administration and management often fall upon people who do not have the training, skill, resources, or interest needed to operate their systems securely.
- The Internet is becoming increasingly complex and dynamic, but among those connected to the Internet there is a lack of adequate knowledge about the network and about security. The rush to the Internet, coupled with a lack of understanding, is leading to the exposure of sensitive data and risk to safety-critical systems. Misconfigured or outdated operating systems, mail programs, anonymous FTP servers, and Web sites result in vulnerabilities that intruders can exploit. Just one naive user with an easy-to-guess password increases an organization's risk.
- When vendors release patches or upgrades to solve security problems, organizations' systems often are not upgraded. The job may be too time-consuming, too complex, or just at too low a priority for the system administration staff to handle. With increased complexity comes the introduction of more vulnerabilities, so solutions do not solve problems for the long term—system maintenance is never-ending. Because managers do not fully understand the risks, they neither give security a high enough priority nor assign adequate resources. Exacerbating the problem is the fact that the demand for skilled system administrators far exceeds the supply.
- There is little evidence of improvement in the security features of most products; developers are not devoting sufficient effort to apply lessons learned about the sources of vulnerabilities. The CERT Coordination Center routinely receives reports of new vulnerabilities. In 1995 we received an average of 35 new reports each quarter. That average has more than doubled in 1996, and we continue to see the same types of vulnerabilities in newer versions of products that we saw in earlier versions. Technology evolves so rapidly that vendors concentrate on time to market, often minimizing that time by placing a low priority on security features. Until their customers demand products that are more secure, the situation is unlikely to change.
- Engineering for ease of use is not being matched by engineering for ease of secure administration. Today's software products, workstations, and personal computers bring the power of the computer to increasing numbers of people who use that power to perform their work more efficiently and effectively. Products are so easy to use that people with little technical knowledge or skill can install and operate them on their desktop computers. Unfortunately, it is difficult to configure and operate many of these products securely. This gap leads to increasing numbers of vulnerable systems.
- As we face the complex and rapidly changing world of the Internet, comprehensive solutions are lacking. Among security-conscious organizations, there is increased reliance on "silver bullet" solutions, such as firewalls and encryption. The organizations

that have applied a “silver bullet” are lulled into a false sense of security and become less vigilant, but single solutions applied once are neither foolproof nor adequate. Solutions must be combined, and the security situation must be constantly monitored as technology changes and new exploitation techniques are discovered.

The next section contains further information about the vulnerabilities of the Internet and thus of the information infrastructure as a whole.

3. Assessment of Internet Vulnerabilities

Because the Internet was not originally designed with security in mind, it is difficult to ensure the integrity, availability, and privacy of information. The Internet was designed to be "open," with distributed control and mutual trust among users. As a result, control is in the hands of users, not in the hands of the provider; and use cannot be administered by a central authority. Finally, the Internet is digital, not physical. It has no geographic location and no well-defined boundaries. Traditional physical "rules" are difficult or impossible to apply. Instead, new knowledge and a new point of view are required to understand the workings and the vulnerabilities of the Internet.

In this section, we give examples of recent malicious attacks on the Internet and examine why the Internet is so attractive to intruders.

3.1 Attack Strategies Illustrating Internet Vulnerabilities

Some attacks are intended to harass a site and deny it the ability to transact business on the Internet. Other attacks enable intruders to gain privileged access to a system so that it effectively belongs to them. With their unauthorized privileges, they can, for example, use the system as a launch platform for attacks on other sites. Still other attacks are designed to reveal sensitive information, such as passwords or trade secrets. We describe three attack strategies below. Our descriptions are neither theoretical nor abstract; rather, they present, at a high level, actual attacks reported to the CERT Coordination Center regularly.[2]

3.1.1 SYN Attacks: Denial of Service

A *SYN attack* is an attack against a computer that provides service to customers over the Internet. *SYN* refers to the type of message (Synchronize) that is used between computers when a network connection is being made. In this attack, the enemy runs a program from a remote location (anywhere in the world) that jams the service on the victim computer. This is known as a *denial-of-service attack* because the effect of the attack is to prevent the service-providing computer from providing the service. The attack might prevent one site from being able to exchange data with other sites or prevent the site from using the Internet at all. Increasingly, companies are depending on Internet services for day-to-day business, from email to advertising to online product delivery. Some companies' business is entirely dependent on the Internet.

[2]All the attacks mentioned in this section are described in CERT advisories, published online by the CERT Coordination Center, Pittsburgh, PA, and available from http://www.cert.org/ and ftp://info.cert.org/pub/cert_advisories/.

SYN attacks have been used successfully against a wide variety of targets, but they have the greatest impact against the companies that provide connections to the Internet. These Internet service providers, or ISPs, provide Internet connection services to government, businesses, and individuals. A SYN attack against an ISP usually results in disruption of Internet service to all the service provider's customers.

This type of attack is very difficult to prevent because it exploits a design flaw in the basic technology used for Internet communication today. Experts are currently working on techniques to reduce the problem somewhat, but preventing these attacks from occurring in the future will require a change in the way Internet communications are accomplished by the computers using the Internet. This is likely to take several years.

3.1.2 IP Spoofing: Masquerading

In an attack known as *IP spoofing,* attackers run a software tool that creates Internet messages that appear to come, not from the intruder's actual location, but from a computer trusted by the victim. *IP,* which stands for Internet Protocol, refers to the unique address of a computer. When two computers trust each other, they allow access to sensitive information that is not generally available to other computer systems. The attacker takes advantage of this trust by masquerading as the trusted computer to gain access to sensitive areas or take control of the victim computer by running "privileged" programs. Information that has been compromised through IP spoofing includes credit card information from a major Internet service provider and exploitation scripts that a legitimate user had on hand for a security analysis.

Unfortunately, there are many computer programs and services that rely on other computers to "speak the truth" about their address and have no other mechanism for disallowing access to sensitive information and programs. The CERT Coordination Center has received many reports of attacks in which intruders (even novice intruders) used this technique to gain access to computer systems with the help of publicly available IP spoofing computer programs.

This attack technique is being addressed by fundamental changes in the way computers communicate over the Internet. The IETF (Internet Engineering Task Force) Proposed Standard for the Next Generation Internet Protocol (IPng) is being designed to provide integral support for authenticating hosts and protecting the integrity and confidentiality of data.

Although early implementations of IPng are underway, the IP spoofing technique is likely to remain effective for years.

3.1.3 Sniffers: Violating Privacy and Confidentiality

For most users of computer networks, including the Internet, the expectation is that once a message is sent to another computer or address, it will be protected in much the same way letters are protected in the U.S. Postal Service. Unfortunately, this is not the case on the Internet today. The messages are treated more like postcards sent by a very fast, efficient pony express. Information (such as electronic mail, requests for connections to other systems, and other data) is sent from one computer to another in a form easily readable by anyone connected to a part of the network joining the two systems together. For Internet data, these messages are routed through the networks at many locations, any one of which could choose to read and store the data as it goes by. The CERT Coordination Center has handled many incidents in which an intruder ran a program known as a *sniffer* at a junction point of the Internet.

The sniffer program records many kinds of information for later retrieval by the intruder. Of specific interest to most intruders is the user name and password information used in requests to connect to remote computers. With this information, an intruder can attack a computer on the Internet using the name and password of an unsuspecting Internet user. Intruders have captured hundreds of thousands of these user name/password combinations from major companies, governments sites, and universities all over the world.

To prevent attacks of this type, encryption technology must be used for both the access to other computers around the Internet (cryptographic authentication) and the transmission of data across the Internet (data encryption).

3.2 Attractiveness of the Internet to Intruders and Attackers

Compared with other critical infrastructures, the Internet seems to be a virtual breeding ground for attackers. Although some attacks seem playful (for example, students experimenting with the capability of the network) and some are clearly malicious, all have the potential of doing damage. Unfortunately, Internet attacks in general, and denial-of-service attacks in particular, remain easy to accomplish, hard to trace, and a low risk to the attacker.

3.2.1 Ease of Internet Attacks

Internet users place unwarranted trust in the network. It is common for sites to be unaware of the amount of trust they actually place in the infrastructure of the Internet and its protocols. Unfortunately, the Internet was originally designed for robustness from attacks or events that were external to the Internet infrastructure, that is, physical attacks against the underlying physical wires and computers that make up the system. The Internet was not designed to withstand internal attacks—attacks by people who are part of the network; and

now that the Internet has grown to encompass so many sites, millions of users are effectively inside.

The Internet is primarily based on protocols (rules and conventions) for sharing electronically stored information, and a break-in is not physical as it would be in the case of a power plant, for example. It is one thing to be able to break into a power plant, cause some damage, then escape. But if a power plant were like the Internet, intruders would be able to stay inside the plant undetected for weeks. They would come out at night to wander through the plant, dodging a few guards and browsing through offices for sensitive information. They would hitch a ride on the plant's vehicles to gain access to other plants, cloning themselves if they wished to be in both places at once.

Internet attacks are easy in other ways. It is true that some attacks require technical knowledge—the equivalent to that of a college graduate who majored in computer science—but many successful attacks are carried out by technically unsophisticated intruders. Technically competent intruders duplicate and share their programs and information at little cost, thus enabling naive "wanna-be" intruders to do the same damage as the experts.

In addition to being easy and cheap, Internet attacks can be quick. In as little as 45 seconds, intruders can

- Break into a system
- Hide evidence of the break-in
- Install their programs, leaving a "back door" so they can easily return to the now-compromised system
- Begin launching attacks at other sites

3.2.2 Difficulty of Tracing Internet Attacks

As we pointed out in the IP spoofing example, attackers can lie about their identity and location on the network. Information on the Internet is transmitted in packets, each containing information about the origin and destination. Again, a packet can be compared to a postcard—senders provide their return address, but they can lie about it. Most of the Internet is designed merely to forward packets one step closer to their destination with no attempt to make a record of their source. There is not even a "postmark" to indicate generally where a packet originated. It requires close cooperation among sites and up-to-date equipment to trace malicious packets during an attack.

Moreover, the Internet is designed to allow packets to flow easily across geographical, administrative, and political boundaries. Consequently, cooperation in tracing a single attack may involve multiple organizations and jurisdictions, most of which are not directly affected by the attack and may have little incentive to invest time and resources in the effort.

This means that it is easy for an adversary to use a foreign site to launch attacks at U.S. systems. The attacker enjoys the added safety of the need for international cooperation in

order to trace the attack, compounded by impediments to legal investigations. We have seen U.S.-based attacks on U.S. sites gain this safety by first breaking into one or more non-U.S. sites before coming back to attack the desired target in the U.S.

3.2.3 Low Risk to Intruders

Failed attempts to break into physical infrastructures involve a number of federal offenses; such events have a long history of successful prosecutions. This is not the case for Internet intrusions. Because attacks against the Internet typically do not require the attacker to be physically present at the site of the attack, the risk of being identified is reduced. In addition, it is not always clear when certain events should be cause for alarm. For example, what appear to be probes and unsuccessful attacks may actually be the legitimate activity of network managers checking the security of their systems. Even in cases where organizations monitor their systems for illegitimate activity, which occurs in only a small minority of Internet-connected sites, real break-ins often go undetected because it is difficult to identify illegitimate activity. Finally, because intruders cross multiple geographical and legal domains, an additional cloud is thrown over the legal issues involved in pursuing and prosecuting them.

3.3 A Note About Loss of Confidence in the Internet

As described earlier, the Internet was designed to survive the disruption of its transport mechanism; but once data was somehow successfully delivered, users believed it to be legitimate. The "internal" attacks now possible enable an intruder to modify programs and configuration files in subtle ways so that they still appear to work. The programs may even appear to be unmodified but will fail under circumstances specified by the intruder. After a successful computer system intrusion, it can be very difficult or impossible to determine precisely what subtle damage, if any, was left by the intruder.

Loss of confidence can result even if an intruder leaves no damage because the site cannot *prove* none was left. With some infrastructures, such as electricity, gas, and emergency services, once an overt denial-of-service attack has been resolved and the service returned, consumers immediately regain trust in the service they receive. But the Internet is highly susceptible to a loss-of-confidence crisis.

Only recently have some vendors begun using a cryptographic technique (checksums) that makes it possible to determine whether files or programs have been modified, and providing features that prevent modification of system files.

In summary, intruders on the Internet continue to prey on the lack of security in many of the products and protocols in use on the Internet today. As the U.S. becomes more dependent on the Internet, the potential impact of a successful Internet-based attack against the U.S.

increases. The next section describes examples of the possible effect of Internet attacks on several critical national infrastructures.

4. The Cascade Effect of a Sustained Attack on the Internet

Sustained attacks on the Internet can undermine other critical infrastructures in a *cascade effect,* the effect that occurs when an attack on one infrastructure causes damage to another. Moreover, it is currently not possible to prevent sustained Internet attacks but only to limit their impact.

In this section, we describe the cascade effect of attacks on the Internet. Damage can occur in a variety of ways. The examples we include are current today, but they also reflect what we expect to see more of in the future.

Historically, many critical national infrastructures were physically and logically separate systems that had little interdependence. As digital information became a more important part of how the infrastructures operated, a "cyber component" of each infrastructure grew. These cyber components are being connected in complex ways as the Internet, intranets,[3] cable television, telephone service, and other information services are becoming interrelated through the physical hardware they use.

The relationships between infrastructures can take many forms. Often one infrastructure uses another as part of its underlying technology. For example, the telecommunications infrastructure relies on the power grid for electricity. It is possible to limit cascade effects by understanding the relationships and compensating for them, taking steps to limit the damage that can cascade from one infrastructure to the other. In the case of the power grid, many critical electronic components of the telecommunications grid are on battery backup to prevent disruption resulting from short-term power failures. In well-understood relationships, limiting factors contribute to the overall health of the infrastructures. In several of the cases discussed below, however, the relationships are not well understood; thus, there is no compensating means for limiting the effect of failure to one infrastructure.

A natural extension of the cascade effect, which we will not discuss here, is the effect of multiple, coordinated, sustained attacks on several infrastructures simultaneously. We leave it to the reader to imagine just how bad things could be if an adversary could control several key infrastructures simultaneously. In this report, however, we focus on the cascade effect of an attack that uses the Internet as a starting point.

Some of the factors contributing to the cascade effect of such an attack are the following:

- The increasingly important role played by the Internet in the national information infrastructure

[3] Intranets are local computer networks that use Internet technology and sometimes use the Internet as a "wire" to connect to other intranets.

- Increased reliance on the Internet as the transport for other networks in the information infrastructure—other critical infrastructures use the Internet to a greater or lesser degree to exchange business, administrative, developmental, and research information between remote sites
- The reliance of other infrastructures on the information infrastructure

The results of the cascade effect include these:

- Infrastructures relying on the Internet will be poorly coordinated and less effective.
- Infrastructures using the Internet as the underlying technology for an operational intranet between remote locations will lose connections.
- Infrastructures supporting both an operational network and Internet connections may expose control of the operational network to attackers, possibly resulting in collapse of the infrastructure.

The sections below give examples of the trend toward increased connections to the Internet. They also outline several ways that Internet-based attacks, or attacks on the Internet, could cascade to other infrastructures.

4.1 Increased Connections and Their Impact

For a variety of reasons, Internet use is increasing at a phenomenal rate. The Internet is being used to support new communications capabilities; and because communicating over the Internet is more cost effective than many other forms of electronic communication, the Internet is also replacing existing communications mechanisms. Below are just a few examples.

The Internet is being used as a solution to the problem of sharing data across the diverse systems that comprise the **emergency services** infrastructure. In response to the need for better coordination during national emergencies, the National Communications System is developing the Emergency Response Link (ERLink) capability [O'Connor 95]. ERLink is designed to use the Internet and other networked services to supply information to all relevant parties during an emergency, including government agencies, hospitals, the Red Cross, and law enforcement. As the Internet proves itself to be a cost-effective method of moving information among emergency service providers, and as these service providers become increasingly dependent on the Internet, any sustained attack on the Internet could have a profound effect on the nation's ability to coordinate across the various organizations that provide emergency services. A sustained attack on the Internet would cause these organizations to revert to using the telecommunications infrastructure, especially fax and phone service, which are far less effective because they do not automate the coordination of many parties simultaneously. Within five years, this fallback position may no longer be possible.

The **medical services** field is rapidly moving to the Internet to coordinate medical advice to local emergency health services nationwide in critical health situations, and even to provide

remote delivery of medical services. For example, some hospitals now use the Internet to coordinate patient transfers in major metropolitan areas. The National Institutes of Health use the Internet to coordinate resources in the research and deployment communities. The Center for Disease Control uses the Internet to alert hospitals to national health risks. Disruption of these services through attacks on the Internet-connected systems, or through denial-of-service attacks on the Internet itself, could have an impact on the delivery of essential health services. In times of emergency or epidemic, the impact could be severe.

Other areas of medical computing are changing rapidly as well**. Patient records** are increasingly maintained in electronic form. Systems such as MEDNET, linking hospitals, doctors, and patients are becoming a critical component of the U.S. health care system [Ghassemi 95]. The Internet is now recognized as a critical part of the national health information infrastructure [Fuller 95]**.** Security for these systems is under investigation (see, for example, the case study performed at Beth Israel Hospital in Boston [McWilliams]). These investigations highlight the potential vulnerability of health records to intrusions on the Internet. Unfortunately, in some cases, this potential vulnerability has already become a reality. In 1993, Detective John Austin of New Scotland Yard reported two cases of electronic tampering of medical records [Austin 93]. One case involved changing the results of cancer tests from negative to positive. The second involved the corruption of brain scan data to be used to guide surgery.

The move to Internet technologies is under way in **transportation**. For example, a major transportation company is using the Internet to control the flow of freight in a mission-critical application. The company uses JAVA with the Internet for connecting customers and suppliers to control the flow of freight through the national transportation infrastructure [Wilder 96]. Other segments of the transportation infrastructure, such as a trucking firm described in *EDI Forum* [Haisting 96], are moving to Internet-based EDI (Electronic Data Interchange) systems to coordinate the transport of liquid and dry bulk materials. For parcel delivery, a major company now depends on Internet technologies to provide information to customers and coordinate delivery resources [Stahl 96]. Simple denial-of-service attacks on these Internet-based applications could disrupt the operation of companies and their delivery of freight. More sophisticated man-in-the-middle attacks that corrupt messages between suppliers, their customers, and transportation brokers could reroute transportation resources to undesired locations or away from areas of critical need. A sustained attack on the Internet that had the effect of altering the content of electronic messages would have a great impact on infrastructures whose well-being relies on those messages.

The **banking and finance** infrastructure is so dependent on computer networks that a successful cyber attack can drastically affect the banking and finance community. The trading markets, electronic funds transfer, and other critical financial functions are currently managed primarily through isolated networks, but this is changing because using shared networks such as the Internet is more cost effective. The CERT Coordination Center staff has visited several financial institutions that use Internet connections to provide information to existing and potential customers. The systems using the Internet do not directly control

financial transactions, but are connected, through firewalls, to networks that also support systems critical to financial transactions. These firewalls are designed to permit some traffic to pass in order to allow maintenance of the Internet-connected systems. Unfortunately, there is no reason to believe that these firewalls are free of security flaws or that the firewalls have been configured in a foolproof way. Though the path from the Internet to the systems conducting financial transactions is probably not straightforward, there is always increased risk when air gaps between systems are replaced by electronics that allow the flow of data and control information.

4.2 Information Infrastructure

When considering damaging effects on critical national infrastructures, we must examine the information infrastructure itself and how it can be affected by a sustained attack on the Internet. The Internet is just one component of the information infrastructure, but an important one. A sustained Internet attack—either in the form of a denial-of-service attack or an attack that gives the adversary control over the operation of critical components of the Internet—can affect not only direct Internet services, such as the World Wide Web or Internet email, but also parts of the information infrastructure that are not directly connected to the Internet in a logical way.

There are several types of relationships through which systems not considered directly connected to the Internet can suffer the cascade effect of an Internet attack. One relationship is that of an intranet distributing critical information and relying on the Internet for the underlying transport. If the Internet experienced a partial or full shutdown, the intranet riding on the Internet (but not logically connected) would suffer degraded or faulty service, resulting in a failure of that portion of the information infrastructure. A sustained denial-of-service attack against the Internet would disconnect a large portion of the information infrastructure and probably bring down the entire infrastructure.

As an example, a major delivery service uses an intranet riding on the Internet to coordinate the delivery of packages [Discovery 96]. If a sustained attack was made through the Internet on the network service providers supporting this intranet, the intranet itself would be shut down, making delivery impossible until the network was restored.

Today there are backup links in the information infrastructure that depend on dial-up access and leased lines; but if the current trends continue, these will be replaced within five years with intranets riding on the Internet. As a result, an attack on one part of the information infrastructure could have a devastating effect on the whole. (Also, the back-up links themselves are susceptible to attack.)

Adversaries who control a portion of the Internet can monitor the networks and activity of organizations without their knowledge. Adversaries can also “spoof,” or masquerade as, legitimate organizations on the Internet; they can issue instructions, demands, threats, or

other messages and make them appear to come from any source the adversaries chose. For example, an alleged cocaine dealer, William Londono, was released from Los Angeles County Jail on August 25, 1987, on the basis of a forged email message [Neuman 95].

Attacks that result in denial of service or control of systems are not the only threats to the infrastructure. Activities that reduce the integrity or privacy of information on the Internet would also be devastating to the information infrastructure as a whole. If there is reduced confidence in the transport of information in the infrastructure, the effectiveness of the infrastructure could be degraded to the point of uselessness. This achieves the same effect as a denial-of-service attack but is much more difficult to recover from.

Reliance on the Internet as the transport for the information infrastructure will grow over the next five years such that, in the absence of change, an attack on the Internet will have a drastic effect on the information infrastructure.

5. Implications for Public Policy

In this section we examine ways in which the government could address issues of network survivability and security. Although no single approach can ensure survivability of the Internet, and thus the information infrastructure, a combination of approaches can reduce the risks associated with the ever-increasing dependence on the Internet and the possibility of a sustained attack on it.

5.1 Context for Public Policy Decisions

In developing Internet-related policy, the problems normally associated with setting public policy are complicated by rapidly changing technology, the unpredictability of the future, and the fact that complicated tradeoffs are involved. The risk that public policy may have adverse effects is much higher than for more mature areas of technology and commerce, and may arise from any of several sources:

- Relying upon insufficient understanding of the sources of the unique value of the Internet
- Placing secondary objectives before primary public policy objectives
- Assuming an analogy with physical world solutions that does not exist
- Failing to consider the inherent global nature of the Internet

The following general recommendations provide the context for the specific recommendations in Section 5.2. These general recommendations provide a foundation for making public policy decisions relating to the Internet and the information infrastructure.

5.1.1 The Information Infrastructure

Treat the information infrastructure as a separate, critical infrastructure. The information infrastructure is a separate infrastructure, culturally, technologically, socially, and physically different from the other critical infrastructures. These differences and the information infrastructure's digital rather than physical nature lead to vulnerabilities that are independent of the other infrastructures.

It is important to develop policies and operational mechanisms that recognize the inherent differences between the physical world and cyberspace. Many of the concepts on which public policy is based do not apply in cyberspace. For example, it is unlikely that effective cybersecurity policy and operations can develop if ideas are based on the more mature, better understood, predictable, and stable context of physical security. Physical security focuses on issues of property damage, loss of life and physical movement, and physical accessibility. In contrast, cybersecurity is concerned with privacy, confidentiality, information integrity, and information accessibility. There is a lack of physical power in cyberspace that imposes a cooperative culture in which the power, leadership, rewards, and successes go to those who are most effective at cooperating and coming to mutual agreements.

Cybersecurity issues also differ because of the immature technology, experimental nature, rapid expansion, and constantly changing use of the Internet.

5.1.2 Cooperating Internationally

Make national policy and operations decisions with the awareness that cybersecurity issues are international in scope and require international cooperation. The information infrastructure lacks the geographic locality necessary for applying the concept of national boundaries and for enforcing or changing regulations at these boundaries. The CERT Coordination Center, for example, has found it both necessary and effective to work with similar organizations in other countries; and recent U.S. Senate hearings on security in cyberspace provide several anecdotes of incidents emanating from or conducted through foreign sites.

As noted above, cooperation and mutual agreement are the rule in cyberspace. To encourage safe practices on the Internet, the U.S. needs to develop policies jointly, cooperate with other jurisdictions, and come to mutual agreements.

5.1.3 Emphasizing Non-Government Needs

Emphasize individual, commercial, and economic needs in public policy, as well as government and military needs. Cybersecurity threats relate directly to issues of privacy, integrity, confidentiality, and denial of service with their attendant financial, social, and loss-of-rights costs to individuals and companies. Cybersecurity policy that neglects these issues is unlikely to satisfy real national needs.

5.2 Specific Recommendations

We offer recommendations for public policy in five areas: reporting and monitoring threats and vulnerabilities, education and security measures for "safe computing," research and development, use of standards, and laws and law enforcement. Each set of recommendations addresses a different aspect of Internet use and security; all help to improve the state of Internet security and ensure that the U.S. information infrastructure is strong.

5.2.1 Reporting and Monitoring Threats and Vulnerabilities

The nature of threats to the Internet is changing rapidly and will continue to do so for the foreseeable future. The combination of rapidly changing technology, rapidly expanding use, and the continuously new and often unimagined uses of the Internet creates a volatile situation in which the nature of threats and vulnerabilities is difficult to assess and even more difficult to predict. To help ensure the survivability of the Internet, and the information

infrastructure as a whole, it is essential to continuously monitor and analyze cybersecurity threats and vulnerabilities. Specific ways the government can contribute are listed below.

- **Designate a single, independent, trusted organization to be responsible for collecting, analyzing, and reporting incident data.** The organization should collect, analyze, and report on quantity, trends, and character of cybersecurity incidents. To obtain the required information, the organization must be well trusted throughout the community. Given the universal concerns about privacy and confidentially and the inherently voluntary nature of reporting, the collection organization should be neither government nor commercial. Nor can it be responsible for public policy, investigation, enforcement, or other activities perceived as conflicting. Organizations that have suffered attacks are often unwilling to discuss their problems for fear of loss of confidence by their customers.
- **Support the establishment of mechanisms for sanitizing and disseminating data on security problems, data that helps the network community understand the scope and cost of the overall problem.** Also needed are programs to increase awareness of security issues and share lessons learned among government agencies and industry. Organizations often are vulnerable because they are not aware of the risks.
- **Share threat information available to the government with the private sector.** This information will help the private sector accurately gauge the threat they face, especially the international threat.
- **Support the growth and use of global detection mechanisms by using incident response teams to identify new threats and vulnerabilities.** The incident response team at the CERT/CC and other response teams have demonstrated their effectiveness at discovering and dealing with vulnerabilities and incidents. Ongoing operation and expansion of open, wide area networks will benefit from stronger response teams and response infrastructures.
- **Encourage Internet service providers to develop security incident response teams and other security improvement services for their customers.** Many network service providers are well positioned to offer security services to their clients. These services should include helping clients install and operate secure network connections as well as mechanisms to rapidly disseminate vulnerability information and corrections.

5.2.2 Education and Security Mechanisms for "Safe Computing"

The population on the Internet has changed drastically in the last few years. The combination of easy access and user-friendly interfaces has drawn users of all ages and from all walks of life. As a result, there are consumers on the Internet who have no more understanding of the technology than they do of the engineering behind other infrastructures. Similarly, many system administrators lack adequate knowledge about the network and about security, even while the Internet is becoming increasingly complex and dynamic.

To encourage "safe computing," there are steps we believe the government could take:

- **Support the development of educational material and programs about cyberspace for all users, both adults and children.** There is a critical need for education and

increased awareness of the characteristics, threats, opportunities, and appropriate behavior in cyberspace. This need goes far beyond protecting children from pornography. It relates to how quickly cyberspace will be developed, to how rapidly and effectively the U.S. will exploit cyberspace to social and economic benefit, and to what influences will drive the economic, social, and political directions in cyberspace.

In particular, support programs that provide early training in security practices and appropriate use. This training should be integrated into general education about computing. Children should learn early about acceptable and unacceptable behavior when they begin using computers just as they are taught about acceptable and unacceptable behavior when they begin using libraries [NRC 91, p 37]. Although this recommendation is aimed at elementary and secondary school teachers, they themselves need to be educated by security experts and professional organizations. Parents need to be educated as well and should reinforce lessons in security and behavior on computer networks.

- **Invest in awareness campaigns that stress the need for security training for system administrators, network managers, and chief information officers.** Building, operating, and maintaining secure networks are difficult tasks; and there are few educational and training programs that prepare people to perform them. Training will also enhance the ability of administrators and managers to use available technology for configuration management, network management, auditing, intrusion detection, firewalls, guards, wrappers, and cryptography.

  Furthermore, the increasing need for such roles in organizations of many sizes and descriptions has led to assigning information security responsibilities to inexperienced personnel with little or no training. In the short term, the greatest need is for short "how to" and "what to be aware of" courses. In the long term, there should be undergraduate-level or master's-level specialties in network and information security.

- **Facilitate the development and deployment of security mechanisms for information in cyberspace.** Security mechanisms can be used to limit the type, quantity, and sources of information that one chooses to receive. Security mechanisms also can be used to limit the audience who will view or change information, to protect privacy, to ensure the validity and authenticity of communications, to protect against intrusions, and to prevent fraud. Security mechanisms enable each party to a transaction (or perhaps parents on behalf of their children or companies on behalf of their employees) to decide what precautions and limitations they desire. In the presence of effective security mechanisms, no transaction will occur without mutual agreement between the parties.

  The mechanisms can be imposed at either the client or server side to limit who gains access to particular information. Security mechanisms can be highly selective and require mutual agreement between the parties before information can be communicated.

Security mechanisms have the added advantages that they do not undermine commerce nor intrude on basic freedoms.

5.2.3 Research and Development

It is critical to maintain a long-term view and invest in research toward systems and operational techniques that yield networks capable of surviving attacks while protecting sensitive data. In doing so, it is essential to seek fundamental technological solutions and to seek proactive, preventive approaches, not just reactive, curative approaches. Specific suggestions are listed below.

- Fund research and development in the areas of security and survivability of unbounded systems' architectures with distributed control. The traditional views of network computing are that systems are fixed in size, components, and structure; that control can be exercised from a central, all-knowing point; and that there is a system administrator who has ultimate authority. These views no longer apply in the world of the Internet. To reap the promise of the evolving infrastructure, ongoing research is needed in the areas of security architectures and models for unbounded domains; techniques that allow development and operation of systems that are robust enough to detect and recover from attacks; techniques and mechanisms to identify, repair, and deploy corrections to flawed software in operational systems; and operational models and mechanisms that allow detection of widespread, distributed attacks, diagnosis of attack techniques, and rapid development and deployment of preventive measures.
- Encourage the development of comprehensive system/security administrators' toolkits. Acquisition and operations organizations should drive the market for comprehensive security toolkits that support network administrators' efforts to operate secure systems. While many tools are available today, these tools do not provide comprehensive solutions to the security problem. Comprehensive toolkits will be developed only when technology users demand them from computer vendors.
- Support the development of techniques for comprehensive, continuous risk identification and mitigation programs. Network operators need guidance in the form of secure network management models, security assessment techniques, and techniques needed for establishing ongoing security improvement programs. These programs must keep pace with rapidly changing threats and technology, must strongly emphasize technology, and must become part of routine practice rather than simple, periodic audits against a static policy.

5.2.4 Use of Standards

> *Successful generally accepted system security principles would establish a set of expectations about and requirements for good practice that would be well understood by system developers and security professionals, accepted by government, and recognized by managers and the public as protecting organizational and individual interests against security breaches and lapses in the protection of privacy.*
>
> —Computers At Risk [NRC 91, p. 27]

The *Computers at Risk* report in 1990 underscored the need for the creation of generally accepted system security principles, to guide system developers and users in deploying systems with some reasonable assurance of safety. Although some principles are now available, none are appropriate for widespread, practical use. Thus, the deployment of systems into the consumer, business, and safety-critical markets continues unabated, while users' ability to compare one system's security against another or against a minimum standard has shown little, if any, improvement. The need remains for a set of minimum security standards for Internet products.

In many security incidents, the CERT Coordination Center staff sees the same problems repeated:

- Systems that are very "trusting" in their out-of-the-box configuration make installation convenient and easy for the end user, but the default settings expose the user to break-ins. The system can be broken into before the owner takes the time needed to reconfigure the system more securely.
- Administrators who look for system records after a break-in find that the security logs they need are turned off by default and no one turned them on after the system was installed. Thus, the compromised sites could neither obtain evidence nor retrieve the information they needed to understand what damage the intruder may have done.
- Administrators trying to recover from a break-in find they have no reasonable way to determine which, if any, of the system files have been modified.
- Security-conscious users who wish to protect their files and sessions online often find that the tools they need are not available by default or that the tools require expertise and special authorization to install or use.

The current situation is not encouraging. Consumers lack awareness and knowledge of technical security issues, and as more homes and businesses acquire computer systems, the median security knowledge naturally decreases. Without concrete guidelines that they can understand, average consumers cannot and do not demand any specific level of security when making purchases.

As a result, vendors do not feel market pressure to provide increased security. Consumers show more concern that systems are easily connected to their existing network and accessible than that they are safe from intruders. The available market choices are thus in the area of price, performance, and ease-of-use features. Consumers, in response, evaluate systems based on these features and work to gain knowledge and expertise in these areas instead of investigating security issues.

In the long term, consumer education (see Section 5.2.2) **is the best means to cause market forces to address this situation. In the short term, generally accepted standards can jump-start the process.** These standards should address areas such as the following:

- Security features should be delivered with more “out-of-the-box” defaults turned on. Users should have to take explicit action to relax security.
- Systems that are capable of being connected to a network should support sufficiently strong authentication to resist attacks that monitor traffic on the network. To assure that the person using the system is who he or she claims to be, systems should support one-time or challenge/response passwords at a minimum, preferably a cryptographically strong authentication mechanism.
- Systems should include support for data encryption of network traffic.
- Security audit logs should be turned on by default with some level of automatic maintenance.
- Mechanisms should be readily available to protect system programs and files from unauthorized modification and/or to detect such modifications.

The Orange Book and related guidelines have had some success in affecting consumer demand and, in response, vendor offerings. Unfortunately, these guidelines are designed to match a security model that is often more appropriate for military needs than private sector needs. Thus, these specifications have not found the widespread acceptance and use needed to improve the minimum level of security that can be expected in systems. Some efforts are underway to develop security models and guidelines more appropriate for the private sector, such as the GSSP (Generally Accepted System Security Principles) and XBSS (X/Open Basic Security Services). However, there are no guidelines currently in widespread use, and it remains to be seen how well they will meet the needs of software developers and users in the coming years.

The government can take the following steps to encourage the use of minimum security standards:

- **Create a policy that government-purchased computers and software must meet a specified set of security standards.** This will have a certain impact directly on the marketplace but ultimately will have a larger impact as an example that the private sector might follow to make similar requirements for their purchases.
- **Include in this policy the requirement for a security alert service that notifies customers of vulnerabilities and repairs.** Some vendors are actively addressing reports of security vulnerabilities in their products, something the marketplace should encourage and reward. Unfortunately, vendors have the impression that a public acknowledgment of problems, even if they have been fixed, reflects negatively on their company. They are concerned that customers will think, “See how many problems this vendor has.” rather than, “See how many problems this vendor has fixed; see how security conscious this company is.” To the extent that commercial acquisition practices are influenced by government procurement practices, the government can promote the latter attitude by requiring a security alert service, thus encouraging vendor acknowledgment of vulnerabilities and announcements of fixes.

5.2.5 Laws and Law Enforcement

In many respects, the Internet and the information infrastructure in general comprise a new patrol area for law enforcement. Unlike the currently recognized jurisdictions based on

geography, cyberspace does not have a central location nor grounding in the physical world. This renders ineffective many of the accepted methods of distributing the job of law enforcement. Our recommended solution is to support our local "cybercops."

Cybercops are law enforcement personnel whose beat is cyberspace. A cybercop must be able to work with law enforcement from other jurisdictions—the criminal will never be found only in cyberspace but in another physical jurisdiction. Cooperation is not limited to the borders of this or any other country; but just as cyberspace spans the entire globe, so must the ability for the cybercop to work with other law enforcement personnel.

It is not effective to make new laws to cover traditional crimes in cyberspace. There are several reasons for this, as the CERT Coordination Center is often reminded through our day-to-day activity. First, creating a new law within the boundaries of the United States is not effective in a jurisdiction that is international in scope. To be effective, any new legislative activity in cyberspace must involve international cooperation. Secondly, the technology is changing faster than laws specific to the technology can change; legislation cannot keep up. Crime certainly will exist using new technology. However, despite the unique characteristics of cyberspace, most of the crimes committed in this environment are traditional in nature, with the use of technology giving a new look to these illegal acts. The most effective way to address traditional crimes is to re-interpret them in the area of cyberspace, not to make new laws.

There are several specific national policies that could help address the international nature of crime in cyberspace:

- **Support our cybercops.** It is important for the U.S. government to support areas of law enforcement responsible for addressing crime on the Internet. Appropriate funding should be allocated to law enforcement agencies to support the training, physical resources, and staff necessary to handle the cybercrimes reported.
- **Ensure that national policy reflects the need of law enforcement to coordinate internationally to solve crimes in cyberspace.** A restriction to handle crimes or pursue criminals only within national boundaries limits cybercops to the areas containing the victims and prevents them from acting where the criminal may be. An early necessary step in developing international cooperation for law enforcement is **to form international hot pursuit agreements** and other fast channels. The U.S. should pursue international agreements that improve the ability of sites, Internet service providers, and law enforcement to investigate and trace break-in activity internationally and in real time (not after the fact). These agreements should include common standards for audit trail data, encryption of investigation communications, names of designated contact persons, and other requirements well known to law enforcement agencies.
- **Ensure that public policy facilitates the widespread use of encryption to protect information and users of cyberspace.** In the experience of the CERT Coordination Center, many of the computer security crimes and incidents on the Internet could have resulted in less damage or been avoided with the personal use of strong encryption. Some of the vulnerabilities exploited by intruders are in programs and protocols fundamental to the Internet; therefore, they cannot be fixed without the widespread deployment and use of cryptographic technology. Standards must be accepted and used worldwide for user-enabled encryption, such as in passwords and email, and for

protocols essential to the basic operation of the Internet, such as DNS (Domain Name Service). Public policy should reflect the need of the citizens of cyberspace to protect themselves from enemies both foreign and domestic.

6. Conclusion

By remembering the inherent differences between the physical and digital worlds, as well as the special risks faced by users of the Internet, the United States government can implement policies that protect individuals and organizations using the Internet for legitimate purposes, improve the security and survivability of the Internet as a whole, and protect the U.S. infrastructures that depend on the Internet from suffering disastrous setbacks or even collapse as a result of a hostile Internet attack.

References

[Austin 93] Austin, John. "Coordinating an Investigation," [panel presentation] . *5th FIRST (Forum of Incident Response and Security Teams) Computer Security Incident Handling Workshop*. St. Louis, Missouri, August 10-13, 1993.

[Discovery 96] Canadian Discovery Channel. "Life on the Internet," episode of the program *Business Security* (first aired December 1996).

[Fuller 95] Fuller, Sherrilynne S. "Internet Connectivity for Hospitals and Hospital Libraries: Strategies." *Bulletin of the Medical Library Association 83,*1 (January 1995): 32-36.

[Ghassemi 95] Ghassemi, H and Wunnava, S. "Development of an Operational Medical Network (MEDNET) Model." *Proceedings of the IEEE Southeastcon '95, Visualize the Future*, New York: IEEE, March 1995.

[Haisting 96] Haisting, L. "Transportation Carriers Use Internet-to-EDI Solutions." *EDI Forum 9*, 3 (1996): 53-57.

[McWilliams 94] McWilliams, S. "How Boston's Beth Israel Hospital Copes with Security on the Internet." *I/S Analyzer 33,* 12 (December 1994): 12-16.

[Neuman 95] Neuman, Peter G. *Computer Related Risks.* New York: ACM Press, Addison-Wesley Publishing Company, 1995, p. 174.

[NRC 91] National Research Council. *Computers at Risk: Safe Computing in the Information Age***.** National Academy Press (1991)**.**

[O'Connor 95] O'Connor, J. and Milligan, V. "An Information Lifeline to the Disaster Area: The Emergency Response Link," 838-841. *Proceedings of MILCOM '95,* Vol. 2. November 1995. New York: Universal Communications.

[Stahl 96] Stahl, Stephanie. "Information is Part of the Package." *Information Week,* No. 596 (September 9, 1996): 206-208.

[Wilder 96] Wilder, Clinton. "JAVA in Gear." *Information Week,* No. 592 (August 12, 1996): 14-16.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY (LEAVE BLANK)	**2.** REPORT DATE **January 1997**	**3.** REPORT TYPE AND DATES COVERED Final
4. TITLE AND SUBTITLE **Report to the PresidentÕs Commission on Critical Infrastructure Protection**		**5.** FUNDING NUMBERS C — F19628-95-C-0003
6. AUTHOR(S) **James Ellis, David Fisher, Thomas Longstaff, Linda Pesante, Richard Pethia**		
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213		**8.** PERFORMING ORGANIZATION REPORT NUMBER **CMU/SEI-97-SR-003**
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) HQ ESC/AXS 5 Eglin Street Hanscom AFB, MA 01731-2116		**10.** SPONSORING/MONITORING AGENCY REPORT NUMBER
11. SUPPLEMENTARY NOTES		
12.A DISTRIBUTION/AVAILABILITY STATEMENT Unclassified/Unlimited, DTIC, NTIS		**12.B** DISTRIBUTION CODE

13. ABSTRACT (MAXIMUM 200 WORDS)

This report was written for the President's Commission on Critical Infrastructure Protection. Based on the experience of the CERT[SM] Coordination Center, we identify threats to and vulnerabilities of the Internet and estimate the cascade effect that a successful, sustained attack on the Internet would have on the critical national infrastructures set out in Executive Order 13010. Finally, we discuss the implications for public policy and make specific recommendations.

14. SUBJECT TERMS: CERT [SM] Coordination Center, critical infrastructures, cyberspace, Internet security, networks, President's Commission on Critical Infrastructure Protection, public policy , U.S. Government.			**15.** NUMBER OF PAGES **30** **16.** PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT UNCLASSIFIED	**18.** SECURITY CLASSIFICATION OF THIS PAGE UNCLASSIFIED	**19.** SECURITY CLASSIFICATION OF ABSTRACT UNCLASSIFIED	**20.** LIMITATION OF ABSTRACT UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. Z39-18
298-102

Emergency Management Assistance Compact (EMAC)

Overview for National Response Framework

EMAC is a national interstate mutual aid agreement that enables states to share resources during times of disaster. Since the 104th Congress ratified the compact, EMAC has grown to become the nation's system for providing mutual aid through operational procedures and protocols that have been validated through experience. EMAC is administered by NEMA, the National Emergency Management Association, headquartered in Lexington, KY.

EMAC acts as a complement to the federal disaster response system, providing timely and cost-effective relief to states requesting assistance from assisting member states who understand the needs of jurisdictions that are struggling to preserve life, the economy, and the environment. EMAC can be used either in lieu of federal assistance or in conjunction with federal assistance, thus providing a "seamless" flow of needed goods and services to an impacted state. EMAC further provides another venue for mitigating resource deficiencies by ensuring maximum use of all available resources within member states' inventories.

The thirteen (13) articles of the Compact sets the foundation for sharing resources from state to state that have been adopted by all 50 states, the District of Columbia, the U.S. Virgin Islands, Puerto Rico, and has been ratified by Congress (PL-104-321).

The four more commonly referenced articles of the compact (Article V, IV, VIII, and IX) address the primary concerns of personnel and states offering and receiving assistance:

Article V - Licenses and Permits
Whenever any person holds a license, certificate, or other permit issued by any state party to the compact evidencing the meeting of qualifications for professional, mechanical, or other skills, and when such assistance is requested by the receiving party state, such person shall be deemed licensed, certified, or permitted by the state requesting assistance to render aid involving such skill to meet a declared emergency or disaster, subject to such limitations and conditions as the governor of the requesting state may prescribe by executive order or otherwise.

Article VI - Liability
Officers or employees of a party state rendering aid in another state pursuant to this compact shall be considered agents of the requesting state for tort liability and immunity purposes; and no party state or its officers or employees rendering aid in another state pursuant to this compact shall be liable on account of any act or omission in good faith on the part of such forces while so engaged or on account of the maintenance or use of any equipment or supplies in connection therewith. Good faith in this article shall not include willful misconduct, gross negligence, or recklessness.

Article VIII - Compensation
Each party state shall provide for the payment of compensation and death benefits to injured members of the emergency forces of that state and representatives of deceased members of such forces in case such members sustain injuries or are killed while rendering aid pursuant to this compact, in the same manner and on the same terms as if the injury or death were sustained within their own state.

Article IX - Reimbursement

Any party state rendering aid in another state pursuant to this compact shall be reimbursed by the party state receiving such aid for any loss or damage to or expense incurred in the operation of any equipment and the provision of any service in answering a request for aid and for the costs incurred in connection with such requests; provided, that any aiding party state may assume in whole or in part such loss, damage, expense, or other cost, or may loan such equipment or donate such services to the receiving party state without charge or cost; and provided further, that any two or more party states may enter into supplementary agreements establishing a different allocation of costs among those states. Article VIII expenses shall not be reimbursable under this provision.

EMAC Governance Structure

An outline of the EMAC Governance Structure is given below:

1. *National Emergency Management Association:* NEMA was established in 1974 when state directors of emergency management first united in order to exchange information on common emergency management issues that threatened their constituencies. NEMA has administered EMAC since 1995 and has 2.5 staff members dedicated to EMAC administration and training.
2. *EMAC Committee:* The EMAC Committee, the managing body of the compact, is a standing committee under the NEMA organizational structure that maintains oversight of EMAC and the EMAC Executive Task Force. The EMAC Committee consists of a chair, fourteen (14) state directors (or their designees) and a non-voting private sector liaison. The emergency management director and Governor from every state and territory that has passed EMAC legislation and signed EMAC into (state) law are invited to participate.
3. *The EMAC Advisory Group:* The EMAC Advisory Group is comprised of invited representatives from the national based organizations who represent the first responder community and other mutual aid stakeholders (including DHS/FEMA, CDC, and the National Guard Bureau). The mission is to facilitate the effective integration of multi-discipline emergency response and recovery assets for nationwide mutual aid through EMAC.
4. *The EMAC Executive Task Force (ETF):* The ETF conducts the day-to-day work of the EMAC Committee. The ETF is comprised of a Chair, Chair-elect, Past Chair, and ten (10) voting Lead State Representative members (chosen by the state emergency management directors), three (3) members at large (chosen by the EMAC ETF Chair), and four (4) non-voting members (NEMA Legal Committee Liaison, NEMA EMAC Coordinator, NEMA EMAC Sr. Advisor, and NEMA EMAC Training Coordinator). The Chair of the EMAC Executive Task Force serves as the Team Leader to the National Coordination Group.
5. *National Coordination Group (NCG):* The NCG (state of the EMAC ETF Chair) works very closely with NEMA on the daily workings of EMAC and during an event works to direct EMAC policy and procedures.

How EMAC Works

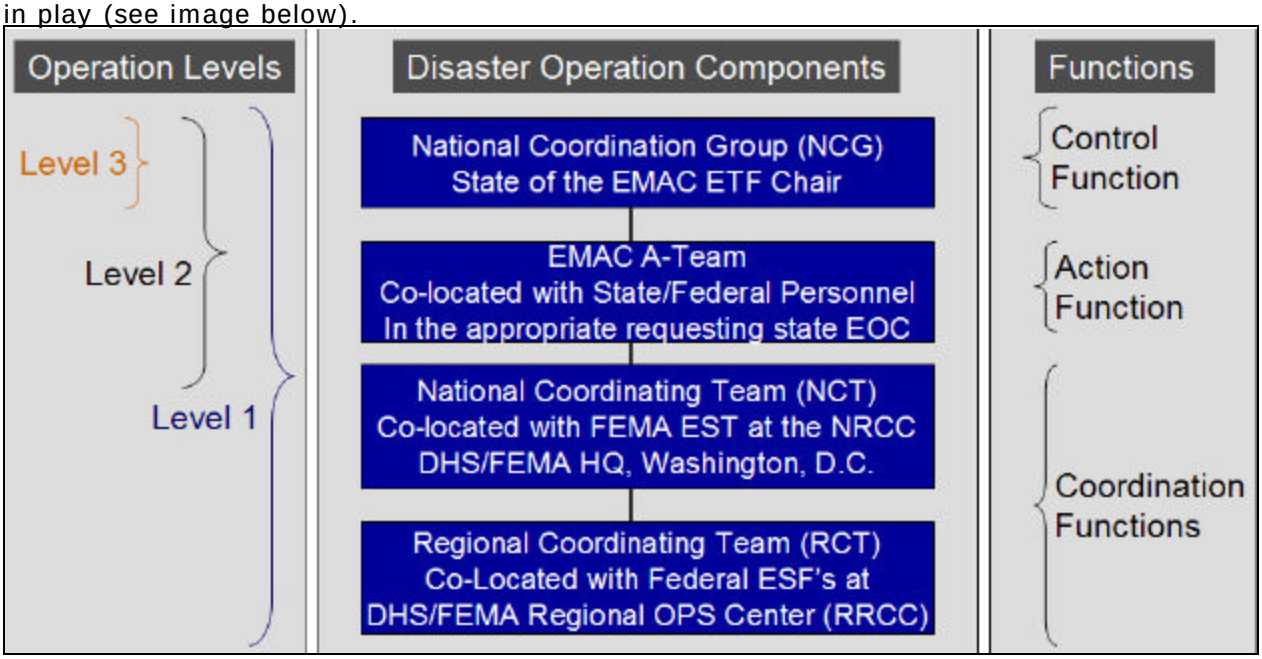
Requesting and deploying resources is made at the discretion of the impacted (Requesting) state allowing them the ability to pick what they need and for what price. The responding (Assisting) state only has to offer assistance if they have the resources and can deploy it. At all times, impacted states retain the choice of seeking resource support from either state or federal, or both as may be appropriate for their circumstances. Local resources can be deployed under EMAC if the state has adopted intrastate legislation (see Model Intrastate Mutual Aid Legislation at NEMA's Web Site (www.nemaweb.org). The EMAC process is outlined below.

> Note: The state emergency management director is an appointed EMAC Authorized Representative and can designate both EMAC Authorized Representatives and EMAC Designated Contacts in their agency. EMAC Authorized Representatives have the authority to obligate the state financially (make requests for resources to come into their state under an emergency declaration). EMAC Designated Contacts cannot financially obligate the state but can be contacted to get more information about EMAC coordination.

1. EMAC Authorized Representative confirms declaration of emergency by Governor
2. State assesses needs for resources
3. State determines if they need an external EMAC A-Team to assist with acquisition of resources or if they will use their in-state EMAC A-Team and acquires external A-Team if needed
4. State determines best source for needed resource (EMAC, Federal, private sector, etc.)
5. EMAC A-Teams request resources by one or all of the following methodologies:
    a. Direct contact with state (knows the resource and can go directly to the state that has it – often a recurring mission).
    b. EMAC resource request is made utilizing the EMAC Emergency Operations System (EOS) broadcast functionality. States may request broadcast by region (FEMA regions), two regions, or 3 regions, an individual state, or an individual EMAC Authorized Representative or EMAC Designated Contact within a state.
    c. Agencies within the states may refer request and suggested resource to the state emergency management agency for their follow-up.
6. EMAC A-Teams determine cost and availability of resources
7. The EMAC REQ-A Form is completed by the EMAC Authorized Representatives between both the Requesting State and the Assisting State.
8. Resources are mobilized from the Assisting State to the Requesting State.
9. Resources check in at state staging areas and are deployment locations and missions are confirmed.
10. Resources complete mission – relaying any issues back to their home state emergency management agency.
11. Resources are demobilized.
12. Assisting States complete reimbursement request and after internal audit sends to the Requesting State.
13. Requesting State reimburses the Assisting State

EMAC Operational Levels

The three levels of EMAC operation (Level 3, Level 2, and Level 1) are mirrored after most state and federal operation levels and have worked effectively and seamlessly within NIMS. The EMAC coordinating components are typed according to size, organizational composition, function, and mission requirements to meet operational demands. EMAC operational deployment levels are activated depending upon the scale of the event. If the event warrants, the levels of operational deployment can be ramped up from a Level 3 to a Level 1. The highest level of EMAC operational level is 1, where all components and functions are in play (see image below).



The decision to expand or elevate the level of operation rests with the EMAC Executive Task Force Chair acting as the NCG Team Leader. The EMAC Operation Levels are reviewed below.

A. Level 3 – The lowest level of EMAC activation involves the activation of the Assisting State, the NCG, and the NEMA EMAC Coordinator. The Assisting State is using their internal state A-Team to request resources.

B. Level 2 – A level 2 operation may involve a single-state or multiple states and deployment of an A-Team is requested by one or more affected states.

C. Level 1 - The highest level of EMAC activation is in effect whenever a single-state or multiple states within single or multiple regions have suffered a major disaster requiring resources. A-Teams have been requested by one or more affected states and DHS/FEMA Headquarters has requested that an EMAC National Coordinating Team (NCT) and/or an EMAC Regional Coordinating Team (RCT) be deployed to appropriate locations to coordinate resource needs with federal and state counterparts.

Infrastructure Interdependencies and Homeland Security

Yacov Y. Haimes

L. R. Quarles Professor of Systems and Information Engineering, and Civil Engineering, and Director, Center for Risk Management of Engineering Systems, Univ. of Virginia, 112A Olsson Hall, Charlottesville, VA 22903. E-mail: haimes@virginia.edu

Introduction

As we can see from the following quotes, infrastructure interdependencies have a strong impact on homeland security.

"The speed, virulence, and maliciousness of cyber attacks have increased dramatically in recent years. More and more people are capable of launching significant assaults against the nation's infrastructure and cyberspace because of the increasing sophistication of computer attack tools. The consequences of a cyber attack on our critical information networks and infrastructures, which are composed of private and public institutions in many different sectors under the guidance of federal-led departments and agencies, can have significant negative effects on the United States" (Dept. of Homeland Security, 2004).

"Our national defense, economic prosperity, and quality of life have long depended on the essential services that underpin our society. These critical infrastructures—energy, banking and finance, transportation, vital human services, and telecommunications—must be viewed in a new context in the information age. The rapid proliferation and integration of telecommunications and computer systems have connected infrastructures to one another in a complex network of interdependence. This interlinkage has created a new dimension of vulnerability, which, when combined with an emerging constellation of threats, poses unprecedented national risk" (President's Commission on Critical Infrastructure Protection 1997).

The quantification of infrastructure interdependencies is central to an effective assessment and management of risks of terrorism to critical infrastructures.

A Need for Research

The advancement in information technology has markedly increased the interconnectedness and interdependencies of our critical infrastructures, including telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services, and continuity of government. There is an emerging need to better understand and advance the art and science of modeling the interconnected large-scale complex economic systems. As quoted above, this need stems from the vulnerability of critical infrastructures to the threats of terrorism.

Historically, many critical infrastructures around the world were physically and logically separate systems with little interdependence. For example, water resource, electric power, and transportation systems, to cite a few, were designed, built, and operated without a threat to their integrity. Today, these and other similar infrastructures have close relationships that can take many forms. These interdependencies and interconnections among infrastructures pose a threat to our society.

To illustrate this complexity further, let us consider the U.S. electric power utility, which is a large-scale, hierarchical, and interconnected system. At the national level, it consists of three main power grids: (1) the Eastern Interconnected System, covering the eastern two-thirds of the United States; (2) the Western Interconnected System, covering the southwest and areas west of the Rocky Mountains; and (3) the Texas Interconnected System, consisting mainly of Texas.

At the network level, each network, as its name implies, is an interconnected system in itself, comprising numerous generators, distribution and control centers, transmission lines, converters, and other elements. Proper functioning of these interacting components is crucial to the continuous operation of the entire power system. In addition to its essential internal dependency, the U.S. power system is externally dependent upon other infrastructure systems, notably telecommunications, fuel supply, and transportation, to name a few.

One significant by-product development attributed to the advancement in information technology has been the reliance of the private and public sectors on supervisory control and data acquisition (SCADA) systems. These systems work remotely to improve the efficiency and effectiveness of the control, operations, and management of critical physical infrastructures. The fact that sectors of the economy and other critical infrastructures are highly coupled renders them at-risk to cyber terrorist attacks. This risk is further exacerbated because they are often remotely controlled and managed through SCADA systems, which are vulnerable to such cyber intrusion. Myriad data collection, control, communication, and management activities, which are essential for the effective operation of large-scale infrastructures, are being performed by SCADA systems.

Since the fundamental purpose of a SCADA system is to control and monitor specific operations (local and/or remote), the need to store business information has added a new function to SCADA: the *management information system* (MIS). MIS enables managers and customers in remote locations to monitor the overall operations and to receive data that allows higher-level business decisions to be made or reviewed. Increasingly, SCADA systems and related technology are replacing and displacing human operators and data collectors in many critical infrastructures. Examples of the functions that railroad SCADA systems are performing include computer-aided train dispatching, underground track heaters for sensors, and control devices. Other systems that are SCADA-controlled include transportation, oil and gas, water, and energy management systems.

To further appreciate the nature of these interdependencies, consider the operation of the electric power system, which is heavily dependent upon voice and data communications. Data

communications provide real-time updates (i.e., every few seconds) of electrical system status to SCADA systems in distribution and bulk electric control centers. Data communications are also used for the remote control of devices in the field, such as circuit breakers, switches, transformer taps, and capacitors. Moreover, data communications allow generating units to follow the real-time signals from the control center that are necessary to balance electricity generation with consumer demand instantaneously. Although the power industry owns and operates the majority of its communications equipment, a substantial portion is dependent on local telephone carriers, long-distance carriers, satellites, cellular systems, paging systems, networking service providers, Internet service providers, and others—all of which are vulnerable to cyberterrorism.

Thus, there is little doubt that in order to ensure the stability, sustainability, and operability of critical infrastructures, it is imperative to fully understand their complexity and interconnectedness, as well as the risk associated with these characteristics. Nonetheless, despite all the research efforts to date, our knowledge about these factors remains limited. In large part, this is because of the daunting complexity involved. Yet it is also because we are still lacking a high-level, overarching framework for modeling interdependencies among large-scale, hierarchical, interconnected complex systems.

Call for Papers

Several groups of researchers in the United States and around the world are responding to the need to better our understanding of complex infrastructure interdependencies. In the United States, teams from the National Laboratories, universities, and the private sector are developing analytical and simulation models with varied levels of success. Although no silver-bullet solution has been developed for this intricate modeling problem, much progress has been made during the last several years to merit the exchange of the state-of-knowledge among these researchers. The *Journal of Infrastructure Systems* will publish a special issue on infrastructure interdependencies and homeland security in 2006. To this end, researchers are encouraged to submit original papers on this theme for this special issue. The complete manuscripts must be submitted to the *Journal* by September 30, 2005. Following the peer review process, authors will be notified on the status of their papers by January 31, 2006.

References

U.S. Dept. of Homeland Security. (2004). "Progress and challenges in security the nation's cyberspace." *OIG-04-29*, Office of the General Inspector, Washington, D.C.

President's Commission on Critical Infrastructure Protection. (1997). "Critical foundations: Protecting America's infrastructures." President's Commission on Critical Infrastructure, Washington, D.C.

Lessons Learned Information Sharing System (www.llis.gov)

Preparedness Directorate
Office of Grants and Training
Tracy A. Henke, Assistant Secretary

Background

Protecting our nation against the threat of terrorism is an increasingly complex mission. Homeland security stakeholders, activities, exercises, and training programs are growing. Everyday, front-line responders at the local, state, and federal levels are creating new and innovative best practices to prevent, prepare for, respond to, and recover from acts of terrorism and other disasters. Exercises and real-world incidents have produced valuable lessons learned for emergency responders—lessons that are often obscured or glossed over in "official" after-action reports. There has been no single resource for responders to effectively share lessons learned and best practices…until now.

Approach

To fill this critical gap, the Office of Grants & Training directed the National Memorial Institute for the Prevention of Terrorism (MIPT) in Oklahoma City, OK to develop the *Lessons Learned Information Sharing* (LLIS.gov). LLIS.gov is a national on-line network of lessons learned and best practices designed to help emergency response providers and homeland security officials prevent, prepare for, respond to, and recover from all hazards, including terrorism. LLIS.gov will enhance national preparedness by allowing response professionals to tap into a wealth of validated front-line expertise on effective planning, training, equipping, and operational practices for homeland security.

Network Features

Secure: All LLIS.gov users are verified emergency response providers and homeland security officials at the local, state, and federal levels. LLIS.gov uses strong encryption and active site monitoring to protect all information housed on the system.

Peer-validated content: The central component of LLIS.gov is a collection of hundreds of peer-validated lessons learned and best practices. These lessons learned and best practices—covering the full range of homeland security disciplines and functions—have been conceived and developed by response professionals for their peers. New content is being generated constantly.

Clearinghouse of information: LLIS.gov serves as a central repository of relevant homeland security documents and events. The system is frequently updated with new reports and publications intended for homeland security personnel. The system houses an extensive catalog of after-action reports (AARs) from exercises and actual incidents and

hundreds of Emergency Operations Plans. Authorized users also have access to an updated list of homeland security exercises, events, and conferences.

Information sharing: The system houses a directory of responders and homeland security officials, allowing users to see contact information for other authorized users. Individuals with functional expertise are identified throughout the system, allowing users to communicate with and learn from those with more experience and proficiency. LLIS.gov also includes on-line collaboration tools including secure email and message boards where users can exchange information.

Self-sustaining network: To sustain and develop the LLIS.gov system, users are constantly encouraged to provide feedback about the system's content through message boards and surveys. Users can also submit potential lessons learned, best practices, good stories, upcoming events, and AARs for inclusion on the system.

For Additional Information

For more information on *Lessons Learned Information Sharing*, please contact the *LLIS.gov* Help Desk at Feedback@llis.dhs.gov

DEC. 05

U.S. Department of Justice
Office of Justice Programs
National Institute of Justice

NIJ

Research in Brief

Public Law 280 and Law Enforcement in Indian Country—Research Priorities

www.ojp.usdoj.gov/nij

U.S. Department of Justice
Office of Justice Programs
810 Seventh Street N.W.
Washington, DC 20531

Alberto R. Gonzales
Attorney General

Regina B. Schofield
Assistant Attorney General

Glenn R. Schmitt
Acting Director, National Institute of Justice

This and other publications and products of the National Institute of Justice can be found at:

National Institute of Justice
www.ojp.usdoj.gov/nij

Office of Justice Programs
Partnerships for Safer Communities
www.ojp.usdoj.gov

NIJ

DEC. 05

Public Law 280 and Law Enforcement in Indian Country—Research Priorities

Acknowledgments

Special thanks to Duane Champagne, Professor of Sociology and American Indian Studies at the University of California–Los Angeles (UCLA), who assisted with methodology issues and arranging funding to support the pilot study. Thanks also to Joe Doherty with the UCLA School of Empirical Research Group, who guided the authors in designing the data collection instrument.

Findings and conclusions of the research reported here are those of the authors and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

This Research in Brief is based on the authors' paper commissioned for the National Institute of Justice (NIJ) Strategic Planning Meeting on Crime and Justice Research in Indian Country, held October 14–15, 1998, in Portland, Oregon. Support was provided by NIJ, with transfer of funds from the Bureau of Justice Assistance, the Office of Community Oriented Policing Services, the Office for Victims of Crime, the Office of Juvenile Justice and Delinquency Prevention, and the Office on Violence Against Women.

NCJ 209839

ABOUT THIS REPORT

Enacted in 1953, Public Law 83–280 (PL 280) shifted Federal jurisdiction over offenses involving Indians in Indian country to six States and gave other States an option to assume such jurisdiction. Affected tribes and States have faced obstacles in complying with the statute, including jurisdictional uncertainty and insufficient funding for law enforcement. Yet, scant research exists on this issue. In 1998 the National Institute of Justice (NIJ) sponsored a review that identified significant gaps in data concerning crime and law enforcement on PL 280 reservations.

What did the researchers find?

Data collection difficulties may hamper future research: Some States and localities may not document response times to reservation-initiated crime reports, and PL 280 data needed from the Bureau of Indian Affairs may be inseparable from statistics for non-PL 280 jurisdictions. Because crime may be unreported or underreported in PL 280 jurisdictions, victimization surveys may be needed to supplement available data on reported-crime rates in these jurisdictions. Research is also needed on:

- Measurable aspects of the quality of State law enforcement under PL 280, such as police response times to crime reports from reservations.
- Documentation of Federal funding and services to tribes in PL 280 jurisdictions, including such factors as jurisdictional vacuums.
- Concurrent tribal jurisdiction and enhancement of State/tribal relationships through cooperative agreements.

Who should read this report?

Federal, State, and local elected officials and policymakers; tribal officials and advocates; law enforcement and other criminal justice professionals, including researchers.

Carole Goldberg and Heather Valdez Singleton

Public Law 280 and Law Enforcement in Indian Country—Research Priorities

This summary is based upon: Goldberg, Carole, and Heather Valdez Singleton, "Research Priorities: Law Enforcement in Public Law 280 States," unpublished paper, Washington, DC: U.S. Department of Justice, National Institute of Justice, October 14–15, 1998, NCJ 209926, available at www.ncjrs.org/pdffiles1/nij/grants/209926.pdf.

About the Authors

Carole Goldberg is Professor of Law at the University of California–Los Angeles (UCLA) and Director of UCLA's Joint Degree Program in Law and American Indian Studies. Heather Valdez Singleton is Research Associate, UCLA American Indian Studies Center.

States lack criminal jurisdiction over crimes committed by or against Indians in Indian country unless Federal legislation expressly grants such authority. Absent that legislation, tribal and Federal law enforcement generally share authority over those crimes, although a realm of exclusive tribal jurisdiction also exists. A significant number of Indian tribes fall under State jurisdiction under Public Law 83–280 (PL 280).[1]

What is Public Law 280?

Congress passed PL 280 in 1953. The statute mandated shifting Federal criminal jurisdiction over offenses involving Indians in Indian country to certain States and gave other States an option to assume such jurisdiction in the future. State jurisdiction over Indians outside Indian country was unchanged.

Retrocession. A 1968 amendment to PL 280[2] contained a retrocession provision enabling a State that had previously assumed jurisdiction over Indians under the law to return all or some of its jurisdiction to the Federal Government, contingent on approval from the U.S. Department of the Interior. The amendment did not permit Indians either to veto State initiatives to retrocede or to impose retrocession

"Indian country" is defined at 18 U.S.C. 1151 as follows:

. . . (a) all land within the limits of any Indian reservation under the jurisdiction of the United States Government, notwithstanding the issuance of any patent, and including the rights-of-way through the reservation, (b) all dependent Indian communities within the borders of the United States whether within the original or subsequently acquired territory thereof, and whether within or without the limits of a state, and (c) all Indian allotments, the titles to which have not been extinguished, including rights-of-way running through the same.

on unwilling States. Subsequent bills to allow tribally initiated retrocession have failed in Congress and State legislatures.

Need for more research. Tribes and States have voiced concerns about some of PL 280's consequences, including perceived jurisdictional uncertainty and insufficient funding for law enforcement. Despite these concerns and the law's importance to Federal Indian policy and law enforcement, little research has been done to determine the law's impact. The authors identified some key areas for future research:

- Quantitative research comparing reported-crime rates in Indian country affected by PL 280 with rates in reservations not so affected and with rates in other parts of PL 280 States.
- Quantitative research bearing on the quality of State law enforcement services under PL 280.
- Documentation and evaluation of Federal law enforcement funding and services

A Current Assessment of Law Enforcement in Indian Country

The National Institute of Justice (NIJ) is currently supporting an investigation of the experiences of Indian tribes and local law enforcement agencies under PL 280. Researchers are studying 17 reservations in 10 States with and without PL 280 jurisdiction. Project objectives are to—

- Compare crime rates on reservations subject to PL 280 with rates on reservations not subject to PL 280.
- Determine the quality and availability of law enforcement and criminal justice under PL 280.
- Evaluate Federal law enforcement and criminal justice funding and services to PL 280 tribes.
- Evaluate retrocession, concurrent jurisdiction, and cooperative agreements as options to alleviate problems in PL 280 jurisdictions.
- Explore possible administrative and legislative responses to PL 280.

The researchers will produce a final report to NIJ and will disseminate relevant data and findings to study participants through teleconferences and written summaries of findings relevant to particular sites. Services will be offered to tribes that request help in drafting documents such as cooperative agreements. Study results are expected by 2006.

to tribes subject to PL 280 jurisdiction.

- Qualitative assessment of law enforcement under PL 280, e.g., examining whether and to what extent jurisdictional vacuums exist.
- Evaluation of the impacts of retrocession and concurrent tribal jurisdiction.
- Review of cooperative agreements in PL 280 States, such as between tribe and State.

A major study sponsored by the National Institute of Justice is investigating some of these areas (see "A Current Assessment of Law Enforcement in Indian Country").

PL 280 highlights

Affected States and tribes. PL 280 transferred Federal criminal jurisdiction in Indian country to six States that could not refuse jurisdiction, known as "mandatory" States (see exhibit 1). The law did not provide for the consent of affected tribes. Thus, criminal laws in those States became effective over Indians within as well as outside Indian country. PL 280 provided no financial support for the newly established State law enforcement responsibilities.

Exhibit 1. States affected by PL 280

Mandatory States[a]	Optional States[b]
Alaska	Arizona
California	Florida
Minnesota[c]	Idaho[c]
Nebraska[c]	Iowa
Oregon[c]	Montana[c]
Wisconsin[c]	Nevada[c]
	North Dakota[c]
	South Dakota
	Utah
	Washington[c]

a. Tribes excluded from State jurisdiction by PL 280 were Confederated Tribes of the Warm Springs Reservation in Oregon and the Red Lake Band of Chippewa Indians in Minnesota.

b. Some of the optional States made their acceptance of PL 280 jurisdiction contingent on tribal or individual Indian consent that was never forthcoming. Other optional States accepted jurisdiction over very limited subject areas.

c. Contains some tribes that have retroceded.

The law also permitted other States, at their option and without consulting tribes, to choose to assume complete or partial jurisdiction over crimes committed by or against Indians in Indian country. Ten States chose to do so; these are referred to as "optional" States (see exhibit 1). In 1968, an amendment to PL 280 required tribal consent before additional States could extend jurisdiction to Indian country. Since 1968, no tribe has consented.

Through PL 280's retrocession provision, several mandatory and optional States have returned jurisdiction over nearly 30 tribes to the Federal government, thereby reinstating tribal/Federal responsibility for law enforcement.

PL 280's scope in terms of affected tribes and Indian population is put into perspective once the broad contours of Indian country are sketched. Federally recognized tribes are spread across 56 million acres in the contiguous 48 States and millions of additional acres in Alaska. Of the 562 federally recognized tribes, more than 330 live in the contiguous 48 States. The U.S. Census Bureau estimates an Indian population of about 2,786,652 (including Alaska Natives), or 0.9 percent of the estimated U.S. population in 2003.[3] All but an estimated 106,450 live in the contiguous 48 States. Almost half of this population does not live on a reservation and is therefore subject to State authority independent of PL 280.

About 23 percent of the reservation-based tribal population in the contiguous 48 States and all Alaska Natives[4] fall under PL 280. The statute covers 28 percent of all federally recognized tribes in the contiguous 48 states and 70 percent of all federally recognized tribes (including Alaska Native villages).

Criminal jurisdiction. Many unusual challenges confront policing in Indian country (see "Overview of Policing in Indian Country"). One is determining criminal jurisdiction, which may lie with Federal, State, or tribal agencies depending on such considerations as the identity of the alleged offender and victim and the nature and location of the offense.

Overview of Policing in Indian Country

Aside from jurisdictional issues, policing on Indian reservations faces many difficulties that law enforcement elsewhere generally need not confront, at least to the same extent. Data collected by the Bureau of Justice Statistics, for example, suggest that violent victimization among American Indians and Alaska Natives exceeds that of other racial or ethnic subgroups by about 2.5 times the national average.[a]

According to a National Institute of Justice-supported study, a typical police department in Indian country serves a population of 10,000 residing in an area about the size of Delaware patrolled by no more than 3 officers at any one time.[b] Even so, many reservation residents live in areas with characteristics of suburban and urban locales. Researchers found that the overall workload of Indian country police departments has been increasing significantly in intensity and range of problems—driven by rising crime, heightened police involvement in social concerns related to crime, and increased demand for police services.

The study reported that most police departments in Indian country are administered by tribes under contract with the Bureau of Indian Affairs (BIA). The second most common type of department management is direct BIA administration. Under the former arrangement, law enforcement personnel are tribal employees; under the latter, they are Federal employees. State and local authorities supply police services to tribes not affected by retrocession in PL 280 States.

Of Indian country police departments surveyed, the researchers found:[c]

Officers that were Native American	66%
Officers that were women	12%
Native American officers who were members of the tribe they serve	56%
Officers who were unable to speak the language native to the community they serve	87%

Notes

a. Perry, Steven W., *American Indians and Crime*, Washington, DC: U.S. Department of Justice, Bureau of Justice Statistics, December 2004, NCJ 203097: iii; 4–6. Violent victimization comprises rape/sexual assault, robbery, and aggravated/simple assault. The report (p. 10) notes that of Indian victims of violent crime who could perceive whether offenders had used alcohol and/or drugs, 71 percent indicated that such usage was a factor in the crimes. That compares to 51 percent for violent crimes against all races.

b. Wakeling, Stewart, Miriam Jorgensen, Susan Michaelson, and Manley Begay, *Policing on American Indian Reservations*, Washington, DC: U.S. Department of Justice, National Institute of Justice, July 2001, NCJ 188095: vi; available at www.ncjrs.org/pdffiles1/nij/188095.pdf.

c. Ibid.: 25.

Exhibit 2 shows how those considerations pertain to criminal jurisdiction in PL 280 States. For example, law enforcement often must consider such questions as: Is the alleged perpetrator or victim Indian or non-Indian? Is the crime major or minor; victimless or not? Did the offense occur in a PL 280 mandatory or optional State?

Court decisions have attempted to define the jurisdictional contours of PL 280; however, they have also raised some areas of uncertainty:

- *Regulatory versus prohibitory laws.* The U.S. Supreme Court has declared that "regulatory" rather than "prohibitory" State criminal laws are outside the scope of jurisdiction conferred by PL 280.[5] This distinction eludes clear definition and has generated considerable litigation.
- *Local versus State laws.* Some judicial decisions reject application of local law to residents of Indian reservations under PL 280.[6] The U.S. Supreme Court

Exhibit 2. Indian country criminal jurisdiction as conferred by PL 280

Offender	Victim	Jurisdiction
Non-Indian	Non-Indian	State jurisdiction is exclusive of Federal and tribal jurisdiction.
Non-Indian	Indian	Mandatory State has jurisdiction exclusive of Federal and tribal jurisdiction. Optional State and Federal Government have jurisdiction. There is no tribal jurisdiction.
Indian	Non-Indian	Mandatory State has jurisdiction exclusive of Federal Government but not necessarily of the tribe. Optional State has concurrent jurisdiction with the Federal courts.
Indian	Indian	Mandatory State has jurisdiction exclusive of Federal Government but not necessarily of the tribe. Optional State has concurrent jurisdiction with tribal courts for all offenses and concurrent jurisdiction with the Federal courts for those offenses listed in 18 U.S.C. 1153.
Non-Indian	Victimless	State jurisdiction is exclusive, although Federal jurisdiction may attach in an optional State if impact on individual Indian or tribal interest is clear.
Indian	Victimless	There may be concurrent State, tribal, and in an optional State, Federal jurisdiction. There is no State regulatory jurisdiction.

Source: U.S. Department of Justice, "Jurisdictional Summary," *U.S. Attorneys' Manual,* Title 9, Criminal Resource Manual 689. Retrieved October 24, 2004, from the World Wide Web: www.usdoj.gov/usao/eousa/foia_reading_room/usam/title9/crm00689.htm.

has not ruled on this question.

- *Concurrent tribal jurisdiction.* Most Federal and tribal justice systems that have addressed the issue of concurrent tribal jurisdiction in PL 280 States have determined that such jurisdiction exists. PL 280 contains no language removing tribal jurisdiction. The U.S. Supreme Court has not ruled on this matter either. But the Office of Tribal Justice, U.S. Department of Justice, concluded in 2000 that "Indian tribes retain concurrent criminal jurisdiction over Indians in PL 280 States."[7]

- *Gaming offenses.* Language in the Indian Gaming Regulatory Act of 1988 suggests that Federal criminal jurisdiction will supersede State jurisdiction in PL 280 States with respect to gaming offenses. That has been contested by several States, including California.[8]

PL 280 did not provide for the consent of affected tribes and did not provide financial support for the newly established State law enforcement responsibilities. It also did not expressly abolish tribal justice system jurisdiction, diminish the Federal Government's overall trust responsibility to tribes, or reject Federal obligations to provide services to tribes other than Federal law enforcement.

Tribal and State concerns

Some tribes have voiced complaints that Federal funding was reduced for decades as a result of PL 280. In recent years, the U.S. Department of Justice has provided funding to tribes in PL 280 States, including funds for victims of crime, violence against women, community-based policing, and court development. Other concerns voiced by PL 280 tribes include the absence of effective law enforcement, infringement of tribal sovereignty, and confusion about jurisdiction when criminal activity has occurred or presents a threat.

State and local law enforcement agencies' criticisms of PL 280 typically focus on the absence of Federal funding for State law enforcement

services within Indian country or on difficulties in carrying out State law enforcement obligations because of uncertainty about the scope of State jurisdiction and officers' unfamiliarity with tribal communities.

Why more research is needed

Empirical research in the criminal justice field tends to focus on Indians as ethnic groups or on Indians in non-PL 280 States.[9] But the shortage of research on PL 280 has not gone unnoticed. A 1998 study funded by NIJ noted the absence of research concerning crime in Indian country in PL 280 States and recommended "a DOJ study devoted to the unique problems of law enforcement on reservations subject to PL 280."[10] Another NIJ-supported study cited "limited research on policing in Indian country" and suggested comprehensive research on law enforcement under PL 280.[11]

Qualitative studies of PL 280's impact. Two major studies that focused on PL 280 have been completed—a 1974 survey of Indians in Washington, an optional State, and a 1995 survey of Indians in the mandatory State of California.[12] Neither study exhausted the research potential of PL 280.

The Washington study's main purpose was to document Indian residents' perceptions of State jurisdiction.[13] About half of the Indians surveyed felt they were treated poorly or indifferently by State, county, or local police. Juvenile matters were of greatest concern to most interviewees. Their next greatest concerns were violent crimes, traffic laws, narcotics, trespass, and theft. Respondents expressed an unusually high degree of uncertainty about the agencies responsible for law enforcement in their tribal territories, and State and local law enforcement personnel seemed equally concerned by the confusion. Whether the problems identified by the study continue to plague Indian country in Washington State is unknown, however, and its single-State focus limits its general applicability to other States.

Part of the questionnaire used in the more recent California-based survey probed tribes' experience and satisfaction with State law enforcement. Tribal concerns about jurisdictional confusion, inadequate or untimely response, and insensitive or discriminatory treatment were evident. Mentioned frequently were problems with drugs and violent crimes. The researchers concluded that limited and uncertain State jurisdiction under PL 280, coupled with the absence of tribal justice systems and law enforcement,[14] created situations where no legal remedies existed. Consequently, tribal members sometimes engaged in self-help that erupted, or threatened to erupt, into violence.

The California study is not a definitive qualitative assessment of PL 280 because of its limited breadth of coverage. Factors affecting tribes in California may have rendered their PL 280 experience atypical and thus not representative of the law's overall impact on PL 280 States.

Quantitative research on PL 280's impact. No quantitative studies of the impact of PL 280 on tribes and local law enforcement exist. Federal, tribal, and State authorities do not compile data needed for such research.[15] For example, most tribes in PL 280 jurisdictions do not report crime data to the Bureau of Indian Affairs' Crime Analysis Division.

For many years, no tribal law enforcement agency under PL 280 jurisdiction responded to FBI requests for crime statistics. That began to change in the mid-1990s as tribes enhanced their law enforcement and justice systems with resources from the U.S. Department of Justice's Office of Community Oriented Policing Services. Still, reporting crime data to the FBI and accessing crime information systems remains a challenge for tribal law enforcement agencies.

The authors have tried with limited success to construct usable crime data for California Indian country. County-level data represent the best

source, but several county sheriffs' offices claim that crimes committed in Indian country often are not reported.

Research priorities

The lack of data on PL 280 presents a serious impediment to understanding the unique set of problems associated with State jurisdiction in Indian country. As noted earlier, there are several areas of concern.

Measuring crime rates. Serious policy analysis must begin by obtaining the best available data on reported-crime rates in Indian country affected by PL 280. To evaluate the impact of State criminal justice jurisdiction compared with the Federal and tribal jurisdiction applicable without PL 280, a desirable approach would be to document the experience in States (mandatory and optional) affected by the statute, States that assumed partial versus complete PL 280 jurisdiction, and States with and without tribal justice systems. These data should be compared with the best crime rate data available from similar reservations in States not affected by PL 280 and with crime rate data for other comparable parts of the PL 280 States.

For particular reservations, comparisons should be drawn between crime data before and after a State's assumption of PL 280 jurisdiction and before and after a State or tribe retroceded jurisdiction under the statute. If data sources are unavailable, documenting the current situation would lay the groundwork for future longitudinal studies.

Because crime may be underreported in a PL 280 State, research on crime victimization is needed. If relevant victimization data are not available, separate surveys should be undertaken.

Measuring State law enforcement response under PL 280. For the same States and time periods noted in the preceding recommendation, researchers should determine the time required for police to respond to crime reports. If State and local law enforcement do not already document response time, the Federal Government should support and fund research to provide the

data. To make appropriate comparisons, documentation of Federal and tribal response times in areas of their jurisdiction is necessary.

Another useful comparison would be the frequency of complaints filed against police by reservation residents in PL 280 States versus those by residents in other parts of those States or by residents of non-PL 280 reservations.

Documenting and evaluating Federal support. The Department of Justice provides direct block grant and formula funds to States. Tribes are eligible to access those resources for law enforcement services. A review of these awards to tribes in PL 280 jurisdictions as subgrantees should assess the degree to which they access those funds and whether funding under some law enforcement programs is systematically denied. For example, researchers at the University of California–Los Angeles (UCLA) conducting a survey of California tribes for the Advisory Council on California Indian Policy estimated that Bureau of Indian Affairs per capita funding for Indians in PL 280 jurisdictions within California was one-quarter to one-half the funding level for all other Indians served by the agency.[16]

Assessing the quality of law enforcement under PL 280. Ideally, the UCLA survey should be replicated and its content amplified for a sample of additional tribes in California, a sample of tribes in other PL 280 States, and a comparison sample of similar tribes in non-PL 280 States and retroceded tribes. Such a comparative assessment across States—administered in an interview format to allow for more open-ended responses—would identify existing strategies and arrangements that may offer more effective law enforcement solutions within the framework of PL 280.

Among the many topics that this survey could address are governmental provision of law enforcement services, the responsiveness of such services, the quality of investigations, the nature and extent of tribal members' understanding of PL 280, identification of jurisdictional vacuums, and views on retrocession.

The qualitative assessment should also interview State and local law enforcement officials involved in carrying out PL 280's mandate in order to determine patrol practices and response times, communication and interaction with tribal communities about law enforcement priorities and practices, funding associated with PL 280 jurisdiction, and how confusion about PL 280 may affect law enforcement practices.

These surveys would provide essential preliminary data and identify problems requiring more intensive study.

Evaluating the impact of retrocession and concurrent jurisdiction. Many tribes dissatisfied with State jurisdiction under PL 280 have responded with retrocession campaigns and development of tribal institutions that can exercise concurrent jurisdiction.[17] Evaluations could identify the reasons for retrocession campaigns; the perceived benefits and disadvantages of retrocession; changes in crime rates since retrocession; and policies and practices at the State, tribal, and Federal levels that contribute to successful retrocession.

Even without retrocession, some tribes have exercised criminal jurisdiction within the framework of PL 280 and limits imposed by the Indian Civil Rights Act. Unlike retrocession, this strategy does not require consent or initiative from the State, although it may require cooperation from Federal funding sources. If research determines that concurrent jurisdiction achieves many of the same objectives as retrocession, tribes in PL 280 States may already possess the means to rectify local problems associated with PL 280. But, apart from legal issues, questions arise about the effectiveness of this approach as an alternative to retrocession. For example, concurrent jurisdiction may engender conflict or competition between State and tribal institutions. Research is needed to determine best practices and methods of allocating law enforcement and prosecutorial responsibility and to identify effective models for cooperative agreements to facilitate concurrent jurisdiction.

Cooperative agreements. Jurisdictional conflicts between States and tribes have engendered bitterness and costly litigation.

Tribal–State agreements may ease such conflicts while supplying needed services to tribal communities within a framework of mutual consent. Research is needed to identify and analyze existing agreements in PL 280 States, assess their value for law enforcement from tribal and Sate perspectives, and suggest possible modifications and improvements. Such agreements can allocate prosecutorial responsibility in a concurrent jurisdiction situation or provide for cross-deputization.

An evaluation of Federal–State agreements should also be included in any comprehensive assessment of potential benefits from cooperative agreements.

Summing up

The research suggested here not only could initiate more systematic and ongoing data collection for crime rates in Indian country subject to PL 280 jurisdiction, but also generate better understanding of the efficacy of State criminal jurisdiction in Indian country. Findings could, in turn, lead to further study to explore possible Federal policies to improve law enforcement within reservations affected by PL 280. Researchers also may want to review the responsibilities of the U.S. Departments of Justice and Interior as well as other Federal agencies that might assist tribes in developing their own justice systems.

Also recommended for review are possible congressional responses, such as legislation clarifying the grant of State jurisdiction, affirming concurrent tribal jurisdiction, encouraging voluntary inter-jurisdictional arrangements between tribes and States under PL 280, or authorizing tribally initiated retrocession.

Notes

1. Act of August 15, 1953, ch. 505, 67 Stat. 588 (codified as 18 U.S.C. 1162, 28 U.S.C. 1360, and other scattered sections in 18 and 28 U.S.C.). Other Federal statutes, enacted before and after PL 280, provided for State criminal jurisdiction over some tribes in some States. Those statutes are not within the scope of this Research in Brief. In addition to granting the affected States criminal jurisdiction over Indian country, PL 280 opened their courts to civil litigation previously possible only in tribal or Federal courts.

2. Act of April 11, 1968, Public Law 90–284, § 403, 82 Stat. 79 (codified at 25 U.S.C. 1323).

3. Population Division, U.S. Census Bureau, Table 4: "Annual Estimates of the Population by Race Alone and Hispanic or Latino Origin for the United States: July 1, 2003" (SC–EST2003–04). Retrieved October 26, 2004, from the World Wide Web: www.census.gov/popest/states/asrh/tables/SC-EST2003-04.pdf.

4. As a result of the U.S. Supreme Court decision in *Alaska* v. *Native Village of Venetie Tribal Government* 522 U.S. 520 (1998), little Indian country remains in Alaska. Consequently, little territory is left in Alaska where the State requires Federal authorization to exercise Indian country jurisdiction.

5. *California* v. *Cabazon Band of Mission Indians,* 480 U.S. 202, 209 (1987).

6. For example, in *Santa Rosa Band of Indians* v. *Kings County,* 532 F.2d 655 (9th Cir. 1975), the Ninth Circuit held that the county could not apply zoning and building codes to tribal land.

7. Office of Tribal Justice, U.S. Department of Justice, "Concurrent Tribal Authority Under Public Law 83–280," position paper, November 9, 2000, available at www.tribal-institute.org/lists/concurrent_tribal.htm.

8. *Sycuan Band of Mission Indians* v. *Roache,* 38 F.3d 402, 407 (9th Cir. 1994), *amended* 54 F.3d 535 (1995).

9. See "American Indian Criminality: What Do We Really Know?" in *American Indians: Social Justice and Public Policy,* Donald E. Green and Thomas V. Tonneson, eds., Madison, WI: The University of Wisconsin System, 1991; Green, Donald E., "The Contextual Nature of American Indian Criminality," *American Indian Culture and Research Journal* 17(2)(1993); and *Native Americans, Crime, and Justice,* Marianne Nielson and Robert Silverman, eds., Boulder, CO: Westview Press, 1996.

10. Lujan, Carol C., James Riding In, and Rebecca Tsosie, "Justice in Indian Country: A Process Evaluation of the U.S. Department of Justice Indian Country Justice Initiative—Final Evaluation Report," Final report for the National Institute of Justice, grant number 96–IJ–CX–0097, 1998, NCJ 181048: 23.

11. Wakeling, Stewart, Miriam Jorgensen, Susan Michaelson, and Manley Begay, *Policing on American Indian Reservations,* NIJ Research Report, Washington, DC: U.S. Department of Justice, National Institute of Justice, 2001, NCJ 188095: 1, 3. Law enforcement under PL 280 was not addressed by this study.

12. Johnson, Ralph W., *Justice and the American Indian,* vol. 1, *The Impact of Public Law 280 Upon the Administration of Justice on Indian Reservations,* Rapid City, SD: National American Indian Court Judges Association, 1974; Goldberg-Ambrose, Carole, and Duane Champagne, "A Second Century of Dishonor: Federal Inequities and California Tribes," unpublished report for the American Advisory Council on California Indian Policy, March 27, 1996 (on file with the UCLA American Indian Studies Library). This study is discussed in Goldberg-Ambrose, Carole, "Public Law and the Problem of Lawlessness in California Indian Country," *UCLA Law Review* 44(1997): 1405, 1437–41;

and in Goldberg-Ambrose, Carole, and Timothy Carr Seward (translator), *Planting Tail Feathers: Tribal Survival and Public Law 280 (Contemporary American Indian Issues No. 6),* Los Angeles, CA: UCLA American Indian Studies Center, 1997. Other studies and assessments have focused on tribal policing but do not address issues associated with State jurisdiction under PL 280 and include a very limited number of PL 280 tribes.

13. The study's staff interviewed approximately 250 members of 20 Washington tribes and Federal, State, and local judicial and law enforcement personnel in the State.

14. Jimenez, Vanessa J., and Soo C. Song, "Concurrent Tribal and State Jurisdiction Under Public Law 280," *American University Law Review* 47(1998): 1627. From pages 1660–61: "With the enactment of Public Law 280, legislators withdrew a significant aspect of the Federal Government's responsibility for law enforcement in Indian country and took their financial support with them."

15. Federal Government studies also have emphasized difficulties in collecting crime data for reservations outside PL 280 States. See U.S. Department of Justice, Office of the Inspector General, *Criminal Justice in Indian Country,* Audit Report 96–16, Washington, DC: U.S. Department of Justice, 1996; also see Wakeling et al., *Policing on American Indian Reservations*: 13–15.

16. See Goldberg-Ambrose and Champagne, "A Second Century of Dishonor." Collecting comparable data for other PL 280 States is difficult because Bureau of Indian Affairs funding is typically distributed by area office, which may cover several States and may not separate data by tribe, even in PL 280 States.

17. See, for example, Bozarth, Bonnie, "Public Law 280 and the Flathead Experience," *Journal of the West,* 39(3)(2000): 46.

The National Institute of Justice is the research, development, and evaluation agency of the U.S. Department of Justice. NIJ's mission is to advance scientific research, development, and evaluation to enhance the administration of justice and public safety.

NIJ is a component of the Office of Justice Programs, which also includes the Bureau of Justice Assistance, the Bureau of Justice Statistics, the Office of Juvenile Justice and Delinquency Prevention, and the Office for Victims of Crime.

Overview of Stafford Act Support to States

This overview illustrates actions Federal agencies are likely to take to assist State, tribal, and local governments that are affected by a major disaster or emergency. Key operational components that may be activated include the National Response Coordination Center (NRCC), Regional Response Coordination Center (RRCC), Joint Field Office (JFO), and Disaster Recovery Centers (DRCs).

1. The Department of Homeland Security (DHS) National Operations Center continually monitors potential major disasters and emergencies. When advance warning is received, DHS may deploy—and may request that other Federal agencies deploy—liaison officers and personnel to a State emergency operations center to assess the emerging situation. An RRCC may be fully or partially activated. Facilities, such as mobilization centers, may be established to accommodate Federal personnel, equipment, and supplies.

2. Immediately after a major incident, tribal and/or local emergency personnel respond and assess the situation. If necessary, those officials seek additional resources through mutual aid and assistance agreements and the State. State officials also review the situation, mobilize State resources, use interstate mutual aid and assistance processes such as the Emergency Management Assistance Compact to augment State resources, and provide situation assessments to the DHS/Federal Emergency Management Agency (FEMA) regional office. The Governor activates the State emergency operations plan, declares a state of emergency, and may request a State/DHS joint Preliminary Damage Assessment (PDA). The State and Federal officials conduct the PDA in coordination with tribal/local officials as required and determine whether the impact of the event warrants a request for a Presidential declaration of a major disaster or emergency. Based on the results of the PDA, the Governor may request a Presidential declaration specifying the kind of Federal assistance needed.

3. After a major disaster or emergency declaration, an RRCC coordinates initial regional and field activities until a JFO is established. Regional teams assess the impact of the event, gauge immediate State needs, and make preliminary arrangements to set up field facilities. (If regional resources are or may be overwhelmed or if it appears that the event may result in particularly significant consequences, DHS may deploy a national-level Incident Management Assistance Team (IMAT).)

4. Depending on the scope and impact of the event, the NRCC carries out initial activations and mission assignments and supports the RRCC.

5. The Governor appoints a State Coordinating Officer (SCO) to oversee State response and recovery efforts. A Federal Coordinating Officer (FCO), appointed by the President in a Stafford Act declaration, coordinates Federal activities in support of the State.

6. A JFO may be established locally to provide a central point for Federal, State, tribal, and local executives to coordinate their support to the incident. The Unified Coordination Group leads the JFO. The Unified Coordination Group typically consists of the FCO, SCO, and senior officials from other entities with primary statutory or jurisdictional responsibility and significant operational responsibility for an aspect of an incident. This group may meet initially via conference calls to develop a common set of objectives and a coordinated initial JFO action plan.

7. The Unified Coordination Group coordinates field operations from a JFO. In coordination with State, tribal, and/or local agencies, Emergency Support Functions assess the situation and identify requirements. Federal agencies provide resources under DHS/FEMA mission assignments or their own authorities.

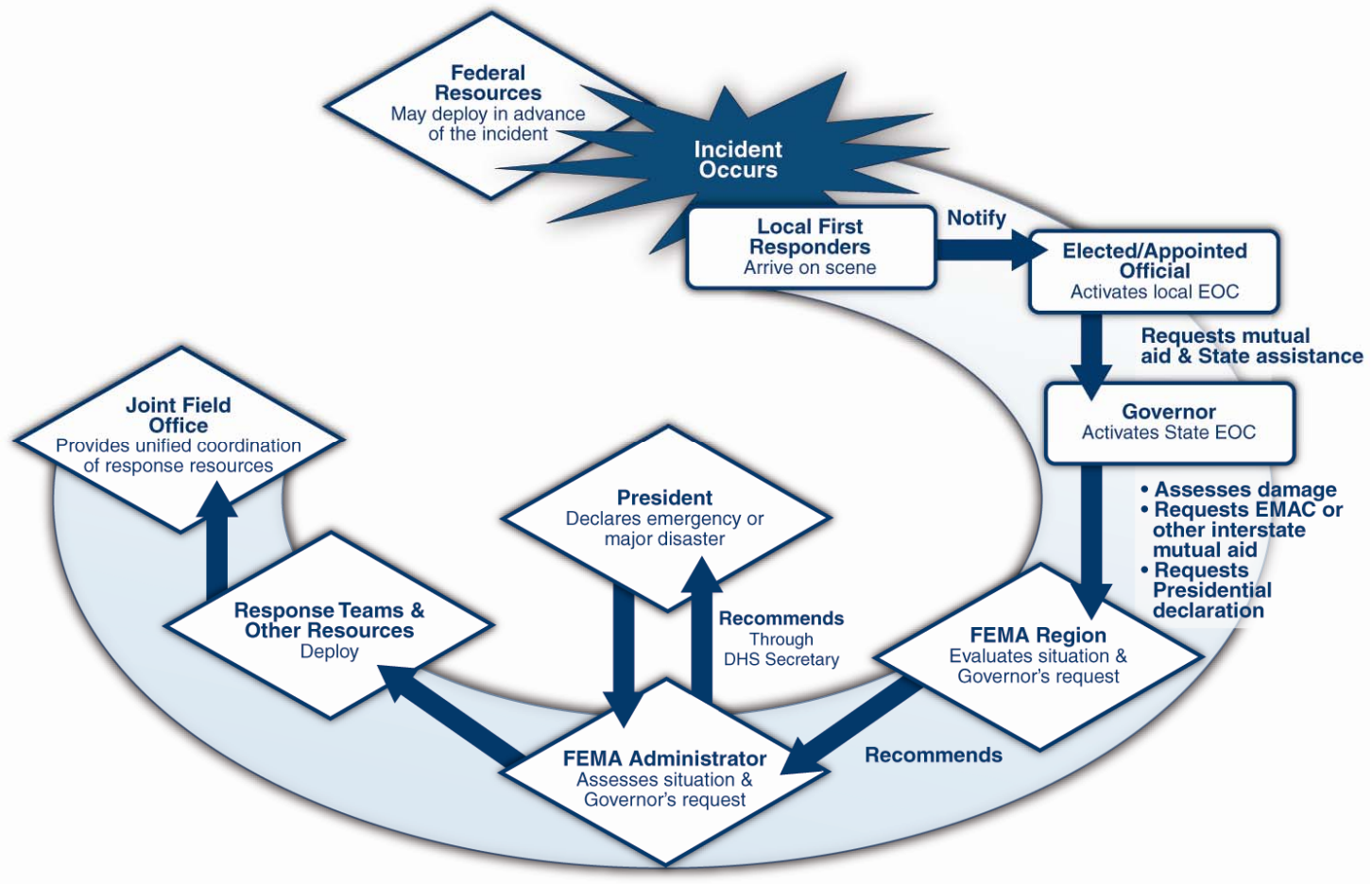
8. As immediate response priorities are met, recovery activities begin. Federal and State agencies assisting with recovery and mitigation activities convene to discuss needs.

9. The Stafford Act Public Assistance program provides disaster assistance to States, tribes, local governments, and certain private nonprofit organizations. FEMA, in conjunction with the State, conducts briefings to inform potential applicants of the assistance that is available and how to apply.

10. Throughout response and recovery operations, DHS/FEMA Hazard Mitigation program staff at the JFO look for opportunities to maximize mitigation efforts in accordance with State hazard mitigation plans.

11. As the need for full-time interagency coordination at the JFO decreases, the Unified Coordination Group plans for selective release of Federal resources, demobilization, and closeout. Federal agencies work directly with disaster assistance grantees (i.e., State or tribal governments) from their regional or headquarters offices to administer and monitor individual recovery programs, support, and technical services.

The following chart summarizes Stafford Act support to States.



How EMAC is Coordinated with the Federal Response:

EMAC is first and foremost a state-to-state compact; however, DHS/FEMA and EMAC leadership have a long-standing agreement in which NEMA, through the NCG, facilitates requests to deploy a team to coordinate EMAC activities with federal personnel whenever requested by DHS/FEMA Headquarters. When requested, this results in EMAC moving from a Level 2 to a Level 1 operation.

Upon a request by DHS/FEMA with the concurrence of the NCG Leader and NEMA, an EMAC Coordinating Team may be deployed to the National Response Coordination Center (NRCC) at DHS/FEMA Headquarters in Washington, DC, or to a DHS/FEMA Regional Response Coordination Center (RRCC). Member States should use Form REQ-B (Appendix V. h: EMAC Forms: 4. EMAC Form REQ-B: NCT and RCT Cost Estimate) to capture estimated mission costs tracked by NEMA.

To stand up the NRCC or an RRCC, FEMA NRCC contacts the NEMA EMAC Coordinator who coordinates with the NRCC, NEMA Executive Director, and the National Coordination Group to complete a task order and determine if the deployment of state resources under EMAC is at a level that coordination is necessitated.

For more information about EMAC visit www.emacweb.org, contact NEMA (www.nemaweb.org), or your state emergency management agency.

Tribal Lands
Homeland Security Summit
At NNALEA's 10th Annual
Training Conference
October 22–24, 2002

NNALEA

NATIONAL NATIVE AMERICAN LAW ENFORCEMENT ASSOCIATION

Tribal Lands Homeland Security Report

National Native American Law Enforcement Association

"Tribal Lands Homeland Security Report"

"Tribal Lands Homeland Security Summit"
at NNALEA's 10th Annual Training Conference
October 22-24, 2002

THE NATIONAL NATIVE AMERICAN
LAW ENFORCEMENT ASSOCIATION

Washington, DC
February 12, 2003

Dear Tribal Lands Homeland Security Summit Attendee and Friends:

We are honored to share this report, which summarizes the proceedings of the National Native American Law Enforcement Association's (NNALEA) "Tribal Lands Homeland Security Summit."

Vital homeland security issues confront American Indian and Alaska Native tribes. The Summit and this report are important first steps and the beginning of an ongoing dialogue amongst a wide variety of interested individuals, agencies and organizations, concerning the vital homeland security issues that confront American Indian and Alaska Native tribes. We, at NNALEA, encourage this dialogue to continue. We recommend that you stay in contact with those you met at the "Tribal Lands Homeland Security Summit" and continue to share your insights.

NNALEA is a strong supporter of tribal efforts to ensure the security of Indian people, tribal lands and resources, and America. NNALEA will continue to provide Native Americans with high quality law enforcement, first responder and homeland security training and technical assistance.

Thank you for taking the time from your many responsibilities and commitments to stand "shoulder to shoulder" with NNALEA in defense of our homelands. Your participation and the sharing of your enthusiasm, knowledge, plans, accomplishments, and ideas made the Summit a success and will make our national homeland secure for our future generations.

Sincerely yours,

David Nicholas,
President
NNALEA

Ronald Reagan Building, International Trade Center • 300 Pennsylvania Avenue Suite 700 • Washington, DC 20004
(202) 204-3065 • Fax (202) 204-3066 • www.nnalea.org

MANY THANKS TO:

Senator Ben Nighthorse Campbell for serving as keynote speaker and a legislative voice for Native American homeland security, to all the attendees who helped develop this "Homeland Security" Report, and to our:

Indian Country "Homeland Security" Summit Sponsors

Department of Justice
Community Oriented Policing Services
Mr. Carl Peed, Director

Bureau of Indian Affairs
Office of Law Enforcement Services
Mr. Robert Ecoffey, Director

NNALEA Executive Board

Dave Nicholas, President
Peter Maybee, 1st Vice President
Dewey Webb, 2nd Vice President
Kim Kraft-Baglio, Sergeant-at-Arms

Daryl Davis, Immediate Past President
Gary Edwards, CEO
Jim Wooten, CFO

Keynote Speakers

Senator Ben Nighthorse Campbell
Chairman, Senate Committee
On Indian Affairs

Neal McCaleb
Assistant Secretary (Indian Affairs)
Department of the Interior

Jacqueline Johnson[1]
Executive Director, National
Congress of American Indians

Thomas Heffelfinger
U.S. Attorney for Minnesota
Chair, AG-NAIS

Other Key Speakers

R. Perry Beaver
Principal Chief
Muscogee (Creek) Nation

Peter Bergin
Assistant Secretary–BDS
Department of State

Daniel G. Bogden
United States Attorney
State of Nevada

Gregg Bourland
Tribal Chairman
Cheyenne River Sioux

Michael Brown
Undersecretary for EP&R
Department of Homeland Security

Bradley Buckles
Director, BATF
Department of Homeland Security

Robbie Callaway
Senior Vice President
Boys & Girls Clubs of America

Gustavo De La Vina
Chief, U.S. Border Patrol
Department of Homeland Security

Robert Ecoffey
Director, BIA–OLES
Department of the Interior

Sharee Freeman
Director, CRS
Department of Justice

Alan Mandell
Chairman
Pyramid Lake Paiute Tribe

Carl Peed
Director, COPS
Department of Justice

(many thanks, continued)

Distinguished Guest Speakers

John Allen
Union Pacific Railway

Andy Ballenger
Department of Homeland Security

M. Christopher Briese
FBI–Minnesota Division

Chris Castillo
El Paso Natural Gas

Mike Derrick
El Paso Corporation

Mark Destito
Drug Enforcement Agency

Dr. Joseph Hessbrook
FEMA

Dr. Scott Hill
Department of Veterans Affairs

Gil Jamieson
FEMA–ONP

John Klein
State of Idaho

Bradley Mahanes
Environmental Protection Agency

Linda Mason
State of Arizona

Sam McCracken
Nike, Incorporated

Jim McLeod
BIA–Homeland Security

Robert Switzer
BATF–Field Operations

Craig Vanderwagen
U.S. Indian Health Service

George Vinson
State of California

Tribal Leader Attendees

Michael Bear
Penobscot Indian Nation

R. Perry Beaver
Muscogee (Creek) Nation

Barbara Birdsbill
Fort Peck Tribe

Gregg Bourland
Cheyenne River Sioux

Robin Burdett
Summit Lake Paiute Tribe

Thomas Christian
Fort Peck Tribe

Carroll Crowe
Eastern Band of Cherokee Indians

Charles Enyart
Eastern Shawnee Tribe

Raul Garza
Kickapoo Tribe of Texas

Carol Ann Heart
Tribal Chairman's Health Board

Darnell Hillaire
Lummi Indian Nation

Pearl Hopkins
Fort Peck Tribe

Brad Levschen
Upper Sioux Community

Alan Mandell
Pyramid Lake Paiute Tribe

Barton Martla
Pueblo of Zuni

Mark Mitchell
Pueblo of Tesuqua

Myron Moses
San Carlos Apache Tribe

Frieda Perkins
Sac & Fox Nation, MO

Herman Shorty
Navajo Nation

John F. Stensger
Colville Tribe IR

Ron Sully
Yankton Sioux Tribe

David Youckton
Chehalis Tribe

(many thanks, continued)

Conference, Summit and Publications Staff

Dawn Abrams
ATF

Nate Alton
U.S. Customs Services

Donny Bulloch
U.S. Secret Service

Gerry Cavis
U.S. Secret Service

Adam Callaway
FirstPic, Incorporated

Chris Chaney
Executive Office U.S. Attorney

Bill Christy
OPM–EMDC

Stephen Cordoza
EMT, U.S. Border Patrol

Herb Drake
BATF–G.R.E.A.T Program

Gilbert Durazo
EMT, U.S. Border Patrol

Amanda Flangas
Nugget Hotel

Jamie French
DOJ–COPS Office

Earl Gardner
DHS–BATF

Ron & Maggie Gurley
BGCA–Green County, Inc.

Luzene Hill
Emory University

Maiby Ho
DHS–INS

Robert Holden
NCAI–Homeland Security

Sherwood "Woody" Lewis
FBI, Retired

Jim Maples
U.S. Secret Service

Rudolph Miranda
U.S. Border Patrol

Doria Moy
DHS–INS

Danny Pierce
U.S. Secret Service

Royleen Ross-Weaver
Helen Keller–ChildSight

Maria Rubio
DOJ–COPS Office

Chuck Sears
U.S. Border Patrol

Anthony "Hoss" Silva
B&CGA–Laguna Pueblo

Matt & Teresa Tate
Oklahoma National Guard

Tracy Toulou
Office of Tribal Justice

Jill Tracy
FirstPic, Inc.

Jim Twoney
U.S. Secret Service

Mary Dawn Verdery
NNALEA Travel Office

Darlene Ward-Reno
NNALEA Budget Office

Ernst Weyand
FBI–Indian Country Unit

Willie Wind
U.S. Secret Service

(many thanks, continued)

Summit Directors, Facilitators & Publication Team

Gary Edwards
Summit Coordinator
Deputy Assistant Director
United States Secret Service

Roger Nisley
President
Eagle International, Inc., FBI (retired)

Francis "Lou" Gros Lewis
Senior Program Analyst/ONAP
Housing & Urban Development

H. Terence Samway
Assistant Director
U.S. Secret Service

Mark Piccirilli
President
FirstPic, Inc.

Jim Wooten
Summit President
Federal Security Director
Transportation Security Administration

Peter Maybee
Assistant Director, BIA–OLES
Department of the Interior

Carol Ann Heart
Executive Director
Tribal Chairman's Health Board

Gary Edwards, II
Attorney
Baker, Donaldson,
Bearman & Caldwell

Dr. Martin Topper
Summit Co-Director
U.S. Environmental
Protection Agency/OCEFT

Jerry Moriarty
Summit Co-Director
Colonel–United Sates Army

Jill Willis
President
Capstone Public Relations, Inc.

Linda Yascowitz
Staff Assistant
NNALEA

Jennifer Garman
Director of Graphic Services
FirstPic, Inc.

Conference Exhibitors

AIS/PRISim Simulators

ATF G.R.E.A.T. Program

Bureau of Indian Affairs

Bureau of Prisons

Community Oriented
Policing Services (COPS)

Department of State

Drug Enforcement Administration

East Central University of Oklahoma

Federal Bureau of Investigations

Galls, Inc.

HUD–OIG

Information Technologies, Inc.

ITT Nightvision

National Criminal Justice
Reference Center

Native American Art

NIJ–Border Research and
Technology Center

NNALEA

Office of Emergency Preparedness

Point Blank, Inc.

Public Health SV USPHS

Second Chance

Smith & Wesson

Social Security Administration

Spillman Tech

U.S. Border Patrol

U.S. Customs

U.S. Immigration and
Naturalization Service

U.S. Mint Police

U.S. Secret Service

Western Community Policing Center

TABLE OF CONTENTS

"Native people are Americans first—and want to stand shoulder-to-shoulder with the rest of their countrymen in defending American lives and homelands from the threats now before us."

"Make no mistake: whether you are a single mom in an urban area, or a family living out in a rural area, you are potentially targeted because you are American."

"From Valley Forge to the war in Afghanistan, Native Americans have heeded the call to defend our country and way of life in numbers greater than any other group in the history of our great nation."

"From many, one. "E pluribus Unum." It has never been more true than now . . ."

". . . by including Indian Tribes in our focus on homeland security, Native communities will stand shoulder to shoulder with the rest of America in defending American lives and homelands against the threats now before us."

A collection of "Homeland Security" statements by
Senator Ben Nighthorse Campbell
Northern Cheyenne Tribe

EXECUTIVE SUMMARY

On September 11, 2001, the threat of terrorism became a reality for Native Americans, as it did for all Americans. The security of the very homeland upon which we all live, was breached. For most of us, this devastating day not only left us searching for answers, but it also left us determined to take steps to reduce the threat that terrorism poses to our homeland in the future.

To address the issue of homeland security in tribal lands, NNALEA hosted the "Tribal Lands Homeland Security Summit" (Summit) at its 10th Annual Training Conference in Reno, Nevada, October 22–23, 2003. The main purpose of the Summit was to bring a wide variety of interested parties together to define the nature of the homeland security threat on tribal lands and to discuss the level of preparedness to meet that threat, now and in the future.

More than 400 representatives of Indian tribal governments, federal agencies, state governments and private industry provided a clear picture of the challenges facing tribal lands. Participants reported potential vulnerabilities, funding restrictions, training deficits, communication challenges, and jurisdictional issues.

Gary Edwards, CEO, NNALEA, reported the Summit findings to the United States Senate Committee for Indian Affairs February 26, 2003. According to Mr. Edwards, "Our nation, as well as Tribal lands, must have a three-part approach to homeland security. We must realize the reality of today, define our vision of homeland security for tomorrow, and act to make that vision the reality of the future."[2]

A reality that must be realized today is that there are certain vulnerabilities on tribal lands that affect the security of not only the Tribal lands but also our Nation as a whole. Specifically, the primary vulnerabilities on Tribal lands today are:

1. the border and port security on Tribal lands;
2. the critical infrastructure located on Tribal lands {i.e., dams, water impoundments and reservoirs, electrical generation plants, drinking water, waste systems};
3. the existence of non-integrated law enforcement and lack of juristictional clarity; and
4. the minimal emergency response, and medical capacity, planning and implementation.

Our vision for homeland security includes a locally-organized grass-roots developed effort, dual-use equipment and services, complementary services funding, adjacent jurisdiction partnerships, special operations training, and "outside the box" thinking.

To make our vision a reality, NNALEA pledges to distribute and update the "NNALEA Homeland Security Assessment Model," continue to provide a forum for the discussion of tribal homeland security, lead in the development of a strategic homeland security defense plan for Tribal Lands, and continue to promote partnerships that facilitate Indian tribes' role in the national homeland defense strategy. Please see Tab 2 for recommendations for support to NNALEA's initiatives.

Senator Ben "Nighthorse" Campbell said it best, "Native people are Americans—and want to stand shoulder-to-shoulder with the rest of their countrymen in defending American lives and homelands from the threats now before us." NNALEA will take its place to provide training, technical assistance, and innovative ways for Native American law enforcement to lead by service to our communities and the United States of America.[3]

SUMMIT PREFACE

The primary result of this nation's search for answers and ways to reduce the terrorist threat was the formulation of the National Homeland Security Strategy, which sets forth three strategic objectives:

1. Prevent terrorist attacks within our homeland;
2. Reduce our Homeland's vulnerability to terrorism; and
3. Minimize the damage and recover from attacks that do occur.

These objectives are to be achieved in six initial areas, as defined by the Office of Homeland Security, namely:

1. Intelligence and warning—to detect terrorism before it manifests itself in an attack:
   a. Build new capabilities through the Information Analysis and Infrastructure Protection Division;
   b. Implement the Homeland Security Advisory System; and
   c. Apply dual-use analysis to prevent attacks.
2. Domestic counter-terrorism:
   a. Improve intergovernmental law enforcement coordination; and
   b. Track foreign terrorists and bring them to justice.
3. Border and transportation security.
4. Critical infrastructure protection
   a. Unify America's infrastructure protection effort;
   b. Build and maintain a complete and accurate assessment of America's critical infrastructures and key assets;
   c. Create effective partnerships with tribal, state and local government and the private sector
   d. Develop a National Infrastructure protection plan; and
   e. Guard America's key assets and infrastructure against "inside" threats.
5. Catastrophic terrorism defense
6. Emergency preparedness and response
   a. Create a national incident management system,
   b. Improve tactical counter-terrorist capabilities,
   c. Enable seamless communication among all responders,
   d. Prepare for NBC contamination,
   e. Plan for military support to civil authorities,
   f. Build the Citizen Corps,
   g. Build a training and evaluation system, and
   h. Enhance the victim support system.

To build on the Office of Homeland Security's initiatives, the Summit targeted five goals that were achieved through the active participation of the attendees. These goals are:

Goal 1: Understanding the threat.

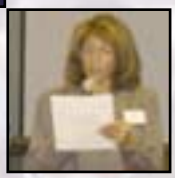
Goal 2: Defining the vulnerabilities.

Goal 3: Identifying resources.

Goal 4: Identifying mechanisms for cooperation.

Goal 5: Defining next steps for moving forward.

The results of each goal are set forth in the remainder of this report.



SUMMIT GOALS
Goal 1: Understanding the Threat

The first goal addressed by the attendees of the Summit hosted by NNALEA was to understand the threat that terrorism poses to our homeland. For Native Americans, and for all Americans for that matter, a good place to gain understanding of the threat of terrorism is the target list of Al-Qaeda, which was determined to be responsible for the September 11 acts of terrorism. This list, which was recently uncovered in a raid, states the following:

- Kidnapping and assassinating enemy (i.e., non-Muslim) personnel, "blasting and destroying the places of amusement, immorality and sin" (i.e., casinos, amusement parks, sporting events, tourist attractions, and the like);
- "attacking vital economic centers" (i.e., dams, power plants, energy pipelines, railroads, ports, radio and television stations, communication towers, etc.); and
- "blasting and destroying bridges leading into and out of the cities."[4]

At first glance, many Americans may conclude that this list, and the threat contained therein, only poses a "small threat" to Native Americans and tribal lands, thereby mistakenly overlooking the much larger threat that this perceived "small threat" poses to our homeland as a whole. A closer look reveals that Native American Lands and Tribal Lands may be at the very heart of the threat to our homeland security. Dams, power plants, energy pipelines, railroads, ports, casinos, and tourist attractions that impact entire regions of our homeland are located on tribal lands. Tribal lands also include many miles of our homeland's border, thereby making them a potential conduit through which terrorism has a means to ingress and egress our homeland as a whole.

Further understanding of this threat was also gained from the remarks provided by several of the speakers at the Summit. Specifically, the remarks by Senator Ben "Nighthorse" Campbell, Neal McCaleb, and Tom Heffelfinger, which are summarized below, detailed the threat of terrorism to Native Americans and Tribal Lands, and the potential impact of such to our homeland as a whole.

Senator Ben "Nighthorse" Campbell

Senator Ben "Nighthorse" Campbell was the keynote speaker at the Summit hosted by NNALEA. Senator Campbell is the Chairman of the Senate Committee on Indian Affairs. He is a Native American and one of the 44 Chiefs of the Northern Cheyenne Tribe. He was elected to the Senate a decade ago, and he is the only Native American to chair the Senate Committee on Indian Affairs. Likewise, he is the only Native American presently serving in the United States Senate.

Senator Campbell referred to the "Tribal Lands Homeland Security Summit" as both "timely and critically important."[5] "September 11th," he said, "brought out the need for coordinated and cohesive delivery of law enforcement, medical response, and security services for all Americans." Senator Campbell discussed the expanding challenges to law enforcement in tribal communities. He referenced how, historically, policing efforts focused on fighting violent crime, domestic violence, theft, and a myriad of problems stemming from alcohol and substance abuse; whereas, in recent years, tribal lands have seen an influx of urban and inner city crimes, such as drug trafficking, gang violence, and illegal immigrant smuggling, which are some of the very activities that finance terrorism.

Senator Campbell acknowledged that our enemies have demonstrated their desire and capability to strike America on its own soil. Like state and local governments, Indian tribes have a vital role in defending our country and our way of life. While some Americans have yet to acknowledge the vulnerability to terrorism in their part of the country, others already convinced of the danger, believe the nation has not begun to address homeland security. Neither is correct.

Senator Campbell provided some examples of federal efforts already under way. These include:

- The National Indian County Telecom Infrastructure Consortium initiative of the Bureau of Indian Affairs. The BIA is working with tribes to coordinate an enhanced telecommunications capacity that will improve tribes' ability to communicate and work with other law enforcement agencies and first responders beyond their borders.
- The Federal Emergency Management Agency (FEMA) is distributing $200 million for state and local hazards emergency planning, development of Emergency Operations Centers, and Community Emergency Response Team Training.
- The Customs Service has adopted a $100 million "Northern Border Strategy" to emphasize securing our long-neglected northern border with Canada. This strategy will combine technology, improved infrastructure, hundreds of new personnel, industry and international partnerships to secure that border. Concurrently, a $10 million security upgrade will be deployed to high volume and high-risk ports of entry on the Southwest border to improve its security also.
- Native American Customs agents, the "Shadow Wolves" are patrolling three million acres of isolated land along 70 miles of Mexican border. They are instrumental in tracking and apprehending smugglers in the American Southwest where no one else can penetrate. The Wolves already are responsible for 70 percent of the 40-60,000 pounds of drugs seized each year by this Customs Service section. Their skills are so valued that the Shadow Wolves have been sent to the Baltics and several former Soviet states to teach others how to identify and track smugglers (of drugs, weapons, people) across international boundaries.
- The Federal Law Enforcement Training Center (FLETC) has increased its support to training Indian Police Officers and now trains over 2,000 officers annually, and
- Through the Bureau of Alcohol, Tobacco and Firearms (ATF) GREAT Program, BIA has trained 214 officers and graduated 28,995 Native Americans from this gang resistance program.

Senator Campbell explained that the Senate Committee on Indian Affairs' commitment to improving the security, living conditions and opportunities for Native Americans is truly bi-partisan. It recognizes that, "Indian tribal law enforcement officers are often the first and only responders to crimes committed against Indians and non-Indians on Indian lands." The Committee has held hearings, and in 2003 will review the practical effect of recent Supreme Court decisions on the ability of tribes to enforce the law on their lands. NNALEA and Summit attendees were encouraged to take part in those discussions, which Senator Campbell views as extremely important to effective protection of the U.S. homeland.

Neal McCaleb

Neal McCaleb was the Assistant Secretary of Indian Affairs for the Department of the Interior at the time of the NNALEA Summit.

Neal McCaleb noted that America's sense of security was shattered by the September 11, 2001 terrorist attacks in New York City and Washington, DC. Echoing the President's frequent call to action, he described the nation as in the midst of "a war on terrorism." Although the challenges of such a war are becoming clear to all, Mr. McCaleb described this as the "best of times" in one sense. The American public has a new respect, appreciation and admiration for those in public safety occupations as well as a strengthened sense of community, cooperation and unity. He described the Summit as an opportunity to share and compare successes and challenges and to prepare to serve and protect those who depend on us.

Tom Heffelfinger

Tom Heffelfinger is the U.S. Attorney for the State of Minnesota and Chairman of Attorney General Ashcroft's Advisory Committee, Native American Issues Subcommittee.

Tom Heffelfinger picked up Mr. McCaleb's theme, adding that this war on terrorism will be the first war in U.S. history that is fought as much by law enforcement and first responders as by the military. He quoted some of the written goals listed in the Al-Qaeda terrorist training manuals, which have been recovered from caves in Afghanistan and raids in the United Kingdom. These manuals urge attacking and destroying vital economic centers such as dams, power plants, energy and transportation centers. Because these terrorists cannot begin to match the nation's military might, they focus on destroying the U.S. economy and our free and open society.

Mr. Heffelfinger believes that the security planning and operations for the Salt Lake City 2002 Winter Olympics should be the model for homeland security public safety operations. He described Olympic security as a "turf free" zone where individuals and agencies gave up their egos and "turf" in the interest of performing a very difficult, dangerous and high visibility mission. While the Secret Service was in charge of planning the security for this National Special Security Event, it needed communication with Olympic organizers, athlete chaperones, intelligence, federal, state and local law enforcement and medical personnel, the military, FEMA and a myriad of other organizations. Procedures for post standing, credentialing, communications, supervision, logistics for housing and feeding law enforcement, security and first responders and an infinite variety of other details required people to work together to make Olympic security successful. The Olympics were confined to a limited area and operated for a reasonably short period of time. These factors made that mission easy compared to securing the American homeland against foreign and domestic terrorists for an indefinite period of time.

Presentation of Colors by U.S. Border Patrol, NNALEA President Jim Wooten, NCAI Executive Director Jackie Johnson, and honored guests.

Jurisdictional procedures and laws should be considered for Tribal Police to become full partners in protecting the homeland. Jurisdictional issues include Tribal Police detaining and prosecuting non-Indians, Tribal Police terrorist training, and cross-deputization agreements.

SUMMIT GOALS
Goal 2: Defining the Vulnerabilities

After the threat of terrorism was understood, the next goal addressed by the attendees of the Summit hosted by NNALEA was to define the vulnerabilities on tribal lands that make all Americans susceptible to that threat. It was determined at the Summit that Native Americans and tribal lands have at least four primary vulnerabilities relevant to the security of our Homeland as a whole. These vulnerabilities, which were consistently reiterated by the attendees of the Summit, are as follows:

1. Border Security;
2. Critical Infrastructure;
3. Integration of Law Enforcement and Lack of Juristictional Clarity; and
4. Emergency Response and Medical Capacity Planning and Implementation.

Each of these vulnerabilities is summarized in more detail below.

Border Security

Twenty-five tribes have land located on or near approximately 200 miles of U.S./International borders. Most of these borders are not adequately patrolled due to limited resources, which make tribal lands, and in turn, our homeland as a whole, subject to undetected terrorist infiltration.

For example, located on one Indian Reservation, there are 76 miles of international border, with numerous unmanned border crossing points. In 2002, the U.S. Border Patrol apprehended 222 illegal immigrants from special interest countries. Even more alarming is the U.S. Customs estimate that numerous undocumented illegal aliens enter our homeland everyday through our borders. Many of these undocumented illegal aliens could be terrorists.

Critical Infrastructure

There are over 100 million acres of tribal and Alaskan Native lands that are replete with dams, water impoundments and reservoirs, electrical generation plants, oil and gas fields/pipelines, transportation lines, and waste systems, among others, that are critical to the infrastructure of our Homeland. A sampling of these resources critical to our infrastructure located on Tribal and Alaskan Native lands are set forth below:

Dams, Water Impoundments, Reservoirs, and Electrical Generation Plants:

- The 2nd largest producer of hydroelectric power in the United States;
- The 4th highest dam in the United States;
- The 12th highest dam in the United States;
- Over 145 other critical dams in located on Tribal and Alaskan Native Lands.

Oil and Gas Fields/Pipelines:

- Oil Fields on many Tribal lands;
- Gas Fields on many Tribal lands;
- Bulk Petroleum Plants on some Tribal Lands;
- Hundreds of miles of pipelines on several Tribal lands;
- Natural Gas Companies on several Tribal Lands.

Transportation Lines:

- Hundreds of miles of railroads run through Tribal and Alaskan Native lands;
- Hundreds of miles of Interstate Highways and many other critical highway systems run through Tribal and Alaskan Native lands.

Others:

- Communication Towers and Water Resources;
- Tourist/Casino Attractions;
- Coal mines, power transmission lines, and slurry pipelines;
- Tourist Attractions on Tribal and Alaskan Native lands are numerous across the United States;

Each of these resources are critical to the infrastructure of our homeland, but each is also a vulnerability should it be compromised by a terrorist attack. For example, one major dam located on an Indian Reservation is over 100 feet high and nearly one mile long. A two-lane highway runs across the crest of the dam, and the dam itself is made of enough concrete to build a 60 foot wide, four-inch thick highway covering the 3,000 miles from Los Angeles to New York City.[6] This dam regulates flood control of a river and forms a large lake, a reservoir and recreational area, holding nine million acre feet of water, and extending 150 miles. The dam's hydro-electric power plant is the largest producer of electricity in the United States, and the third largest in the world. It is the major supplier of electricity to a large number of states. The 6.5 million kilowatts annual generation capacity equates to $130 million of power at wholesale levels. It also irrigates more than one-half million acres of otherwise arid land,[7] and forms the a national recreation area, which contains a seasonal habitat for 24 Bald Eagles, seven scenic and historical trails, and fishing areas. Tourist business provides millions of dollars and hundreds of jobs to the local economy and small business owners.

With the background of the above described major dam in mind, the effects of a successful terrorist attack on it are easily conceivable. Such effects could include loss of power (brownouts or blackouts) for citizens, businesses, hospitals and government agencies in several states; flooding (of a major United States City as well as other smaller cities and communities) and loss of thousands of lives (both people and animals) in communities and businesses situated in the major river's flood plain;

This dam's hydroelectric power plant is the largest producer of electricity in the United States, and the third largest in the world.

and, the development of filth-based diseases such as cholera due to human and animal cadavers and the flooding of sewage systems. The down river destruction of other dams could multiply this devastation. Hundreds of millions, perhaps billions, of dollars in property and business destruction could be expected, in addition to the cost of rebuilding the massive dam.

Integration of Law Enforcement and Lack of Jurisdictional Clarity

Many Native American communities do not have formal agreements with local, state, and federal officials regarding law enforcement, which has created gaps in safeguarding tribal lands, critical resources located thereon, our

homeland as a whole, and all Americans, Native American and non-Native American alike.

"At the onset, every disruption or attack is a local problem. Regardless of who owns and operates the affected infrastructure, each requires an immediate response by local authorities and communities who must support the initial burden of action before the incident escalates to a national event."[8]

State and local jurisdictions should enter into mutual support agreements with Indian nations to share complementary resources in times of crises. In addition, state and local governments should be encouraged to enter in cross deputization agreements to facilitate the mutual sharing and support of peace officers, particularly in times of crises. These cross deputization agreements should provide certified Indian Police officers equivalent status as all other police departments.

Jurisdictional impediments will need to be removed for tribal police to become full partners in protecting the homeland. Both procedures and laws will require changes. For example, tribal police and tribal courts must have broader authority to detain and prosecute Indians and non-Indians committing crimes on Tribal lands. These changes will make tribal law enforcement more effective and aid to close the parity gap in law enforcement between Tribal communities and non-Tribal communities.

Emergency Response and Medical Capacity Planning and Implementation

Communities look to local leadership to assure safety, economic opportunities and quality of life. Public confidence, therefore, starts locally and is dependent upon how well communities plan and are able to protect their citizens, respond to emergencies, and establish order from chaos. Local communities play critical roles in preparing their citizens for emergencies and engaging their public and private leadership in the development of coordinated local and regional plans to assure the protection of residents and businesses.[9]

The Federal Emergency Management Agency (FEMA) is distributing $200 million for state and local hazard emergency planning, development of Emergency Operations Centers, and Community Emergency Response Team Training. FY-2002 funding was provided to states on the basis of population alone. Summit participants believe that funding should be prioritized and provided to both states and tribes according to a risk model based on the need for basic emergency response staffing and infrastructure.

FEMA expects that FY-2003 funding will be allocated by a formula that will provide a set amount of base funding to each state. Funding above this base will be allocated based on population. Therefore, without legislative intervention, tribal lands do not appear to be in line for direct funding for FEMA support until FY-2004 at the earliest.

Current funding for tribal law enforcement and first responders lags well behind that for non-tribal law enforcement and first responders. The result is that many Tribal law enforcement and first responder programs lack personnel, and the personnel they do have may need training, education, certification, experience, and sufficient technical assistance, while many experience burn-out resulting in low retention rates. Therefore, the cost will be higher to attain parity in law enforcement and first responder programs on Indian lands.

According to Senator Campbell, "Indian tribal law enforcement officers are often the first and only responders to crimes committed

against Indians and non-Indians on Indian lands." In addition, Tribal lands have critical unmet needs for medical capacity, emergency response planning, and emergency service implementation.

For example, Tribes are looking more and more to the private sector for health care services that the Indian Health Service does not have the resources to provide. In addition, one Tribal Nation employs only four full-time emergency managers to provide technical and short-term planning assistance to 110 units of local government, covering an area the size of West Virginia. On this same reservation, the Tribe employs only eight full-time fire and rescue staff to serve a population greater than 250,000. Due to inadequate funding, most fire emergency response services are provided by volunteers.

In oral remarks at the Indian Health Service, National Councils Combined Annual Conference, a senior Indian Health Service official made the following statements regarding funding levels in the Indian Health Service 2004 budget for Indian Health Programs:

- As a provider, I know that there will be some (health) services I can provide and others that will have to be delayed or denied.
- The (2004) budget includes $25 million for Contract Health Costs, an amount that will support the purchase of approximately 511,000 outpatient visits, an increase of 17,000 from FY 2003.
- Almost 8 percent of Indian homes still lack a safe indoor water supply, compared to 1 percent of all U.S. homes.

If a weapon of mass destruction was used in a terrorist attack on or near a reservation, resource limitations like those described above would effect emergency response, communication, transportation, public works, firefighting, health and medical services, information analysis, urban search and rescue, the proper identification and containment of hazardous materials, food and water availability, as well as energy supply, public safety, and clean-up. All these elements listed need to be coordinated in a pre-planned organized manner on Tribal lands.

With respect to Tribal coordination with emergency assistance from federal agencies, the Department of Health and Human Services (HHS) is the primary agency responsible for the health and medical response under FEMA's Federal Response Plan. The Department of Health and Human Services is prepared to respond to terrorist attacks on a national basis. The HHS Center for Disease Control (CDC) coordinates the building of the Health Alert Network (HAN) and the National Electronic Disease Surveillance System (NEDSS). Both programs are next generation national public health communications and disease surveillance programs utilizing internet connectivity.

However, tribes may have trouble integrating their response activities with such sophisticated systems because of infrastructure limitations. Almost a quarter of rural Native Americans lack basic telephone service and 8 percent lack a safe indoor water supply. The Indian Health Service must purchase over 500,000 outpatient visits from the private sector, and some health services for Tribal people will either have to be delayed or denied. Given these disparities, homeland security preparedness would dictate that funding for Tribal emergency response, medical capacity planning, and implementation programs should be reevaluated, and access to adequate funding for basic infrastructure support be made available.

. . . this war on terrorism will be the first war in U.S. history that is fought as much by law enforcement and first responders as by the military.

United States Attorney
Tom Heffelfinger
NNALEA Summit Report
Page 5

SUMMIT GOALS
Goal 3: Identifying Resources

The third goal pursued and achieved by attendees of the NNALEA Summit was to identify the resources of Native Americans relevant to homeland security. This goal is very important, as it takes resources to safeguard vulnerabilities from attack by terrorists. Accordingly, at the Summit, attendees were requested to help identify both the resources available to Native Americans on tribal lands to safeguard against the vulnerabilities identified in Goal 2, set forth above, and those resources that are needed by Native Americans to safeguard tribal lands, and our Homeland as a whole. The results of the identification of the available resources, and the needed resources are each discussed in more depth below.

Available Resources

1. **Tribal law enforcement and first responder services.** A large number of Indian nations do have tribal law enforcement and first responder services. NNALEA has provided national training for tribal lands law enforcement professionals for the last 10 years. In addition, in 2002 NNALEA presented the "Tribal Lands Homeland Security Summit" and NNALEA is in the process of coordinating the development of the "Academic Center for Excellence in Native American Law Enforcement Training."

2. **Private Industry.** At the Summit hosted by NNALEA, the Union Pacific Railroad, El Paso Natural Gas Corporation, homeland security and emergency management officials representing companies with holdings in many states made presentations on their security efforts and how they interact with Indian Nations. The Union Pacific representative detailed how the railroad industry responded after the terrorist attacks of September 2001. The railroad industry, like the airlines, shut down. Railroads ceased operating for 72 hours while engineers, police and security officials examined every major structure, bridge, fueling station and other vital structures. Within a month, the Union Pacific determined that it had 265 tunnels, 762 bridges, 138 fueling centers and 33 data distribution centers among its vital structures.

The industry adopted four states of heightened alert—near normal; heightened; credible threat; and confirmed threat/actual attack. Within each of these states, specific security enhancements were defined and agreements were made with federal, tribal, state and local officials for necessary public safety assistance. The railroad industry also formed five Critical Action Teams around the five core functions related to terrorist threats: hazardous material transportation and storage, operations security, critical infrastructures, information technology, and military liaison.

El Paso Natural Gas has $47 billion in annual revenue and 14,000 employees. It owns 48,000 miles of natural gas pipelines, 95 power generating stations, 21,000 miles of gathering pipelines, slurry lines, and oil drilling platforms. Its pipelines cross six states and 12 tribal nations. Its pipelines are monitored around the clock for flow and pressure, and emergency response crews are on stand by. The safety of its employees, customers, and citizens near its right of ways is of primary importance to the company. In addition to automated monitoring, El Paso checks its pipelines by helicopters, ground vehicles

and foot patrols. Like Union Pacific, it has extensively tested and improved its emergency response plans. It also relies on Indian Nation resources for security and public safety protection during emergencies and potential emergencies. For example, the Gila River Indian Police recently provided security at an El Paso facility, pending arrival of the company's emergency response personnel.

3. **California State Security.** At the NNALEA Summit, California Governor Gray Davis' Special Advisor for State Security briefed the conferees on how the nation's most populous state approaches homeland security. He informed us that the state health department was now closely integrated with California's security planning. He believes the anthrax killings opened eyes to the notion that homeland security requires more than security professionals. As a former supervisory agent with the FBI, he believes that terrorists are nothing more than criminal enterprises which employ fanatical and suicidal agents. The same steps law enforcement has applied to shutting down criminal enterprises will ultimately work against terrorists. This makes the war of terrorism a winnable one, although it might take some years to bring to a close.

4. **Arizona Division of Emergency Management and Military Affairs.** At the NNALEA Summit, the head of the Arizona Division of Emergency Management and Military Affairs discussed her efforts to integrate Arizona's 22 tribes into the state vulnerability and risk assessment process. She explained that Arizona is a "delegating state" that pushes resources and responsibility to the county level for program implementation. After the state's first iteration of offering workshops to community leaders and first-line domestic preparedness officials, only 50 percent of cities and towns and 23 percent (5 of 22) of the Indian Nations had received training. Communication from the state to these governments was identified as the reason for the low rate of training participation. After making some improvements to that process, 80 percent of cities and towns and 55 percent (12 of 22) Indian Nations had received training by the end of the program's second year.

5. **Idaho Emergency Preparedness Program.** At the Summit hosted by NNALEA, the head of Idaho's Emergency Preparedness Program explained that emergency planning doctrine recognizes 10 key hazards: agricultural; arson; assassination of high profile personnel; biological; chemical; cyber; explosives, narcotics, nuclear and radiological terrorism.

6. **Border Patrol.** The Border Patrol's mission is to secure and protect the external boundaries of the United States, preventing illegal entry and detecting, interdicting and apprehending undocumented entrants, smugglers, contraband and violators of other laws. There are 8,000 miles of U.S. borders to patrol including 4,000 miles of northern border with Canada, 2,000 of southern border with Mexico, and 2,000 of coastal borders. The Border Patrol divides itself into 21 sectors throughout the United States. Indian reservations are part of 12 of those 21 sectors. Besides the Border Patrol, there are few law enforcement resources along the borders beside the Indian Police Officers. The relationship that has been established with Native American

Border Patrol Chief Gustavo De La Vina and Summit participants view a Border Patrol Surveillance Helicopter.

law enforcement and the U. S. Border Patrol is a valuable conduit in detecting and apprehending illegal immigrants.

7. **Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF).** The ATF, and about 90 percent of its personnel, are moving from the Department of the Treasury to the Department of Justice. This is part of the same government reorganization which created the Department of Homeland Security. "Explosives" has been added to the agency name, reflecting its long history in regulating explosives and investigating bombings. The agency will continue to use the ATF moniker.

"The Spirit of Cooperation"—Actor/Singer Branscombe Richmond, Border Patrol Officers, and a Bureau of Alcohol, Tobacco, Firearms and Explosives Incident Response Vehicle.

Five to six billion pounds of explosives are used lawfully in the United States each year. Regulating that volume is a huge task. ATF is the primary Federal agency responsible for responding to fires, bombings and explosives incidents.

Fighting Terrorism is the number one priority of the ATF. Suppressing black marketing in cigarettes is an important facet of the war on terrorism. Many states have raised taxes on cigarettes as a way to discourage people from smoking as well as a method of raising revenue. As a result, a lucrative black market has arisen in trafficking cigarettes. More particularly, cigarettes are purchased at cheap prices in tobacco growing states then transported by truckloads to industrial states where prices and taxes are much higher. States including Kentucky, Oklahoma, North Carolina and Texas are part of a crime pattern that directly supports terrorism. In a recent case, ATF traced the purchase of cigarettes in North Carolina to their delivery to the black market in Detroit, Michigan. The money from that transaction was traced to the Hezbollah Middle Eastern terrorist group.

Project Safe Neighborhood, an integrated violence reduction program that removes violent criminals from society, is the second highest priority of ATF. United States Attorneys throughout the United States are a vital part of the program. They make prosecuting violent offenders, and getting them the longest sentence allowable, a high priority in their offices.

8. **Bureau of Indian Affairs (BIA).** The BIA warned that homeland security funding must be both cost effective, based on risk management methodology (similar to the design included in the NNALEA Homeland Security Assessment Model) and linked directly to the National

Senator Ben Nighthorse Campbell Chairman, Senate Committee On Indian Affairs.

Homeland Security Strategy. Summit participants were urged to design, create, and implement holistic programs that embody improved communication and cooperation throughout the various levels of government.

The BIA commented that many tribes are located on or near international boundaries and waterways. Casinos, dams, communications towers and other infrastructure

are viable targets of the type terrorists prefer. Recently, an attempted kidnapping was foiled on the Passamaquoddy Indian Reservation. This incident and the examples NNALEA has presented in this report provide "hard evidence" that terrorist threats apply as much to tribal lands as to any other part of America.

The BIA is developing a database of tribal points of contact for homeland security issues. It hopes to make this information available in the Internet. Several issues will be addressed by Department of Homeland Security working groups. These include: information and intelligence sharing and plans for addressing border vulnerabilities, digital connectivity, funding equity and operations security issues. BIA believes that DHS must and will receive tribes as equal partners in deciding how best to protect the American homeland.

9. Drug Enforcement Agency (DEA). The DEA has 200 offices in the U.S. and 70 offices worldwide in 56 different countries. Its principal role in homeland security is the suppression of narco-terrorism. The DEA offers classes to law enforcement officers in how to respond to methamphetamine labs. This class has great applicability to dealing with bioterrorism and is essentially a mini Hazardous Materials (HAZMAT) class. DEA also offers a longer clandestine laboratory certification course at its headquarters in Quantico, Virginia. This is important because prior to the U.S. campaign against Al-Qaeda and the Taliban government, Afghanistan produced 70 percent of the world's opium supply. The sale of narcotics internationally was a significant means of funding terrorist activities. The drugs most often abused in the U.S. are methamphetamines, including pseudo ephedrine, its precursor. In addition, the nexus between drugs and terrorism has led the DEA to begin asking separate lines of questions dealing with terrorist plans and activities. These questions have been added to its existing list of drug related questions that it asks its operatives and prisoners. Information gathered from the debriefings is shared throughout the intelligence and law enforcement systems.

10. Environmental Protection Agency (EPA). The mission of the EPA is to protect human health and the environment. Chemical attacks by terrorists may first present themselves as hazardous material incidents. EPA maintains a national counter-terrorism evidence response capability as well as a national environmental forensic center with expertise in radiological and chemical weapons of mass destruction. It also has emergency response programs, drinking water protection programs, and chemical industry regulatory functions that are vital to homeland security. EPA has a criminal enforcement program that focuses on prevention and training as well as the investigation of environment crimes.

EPA maintains a smooth working relationship with Indian nations and tribes on a government to government basis. It has many grants and agreements with tribes and provides training, technical expertise and other assistance, as requested. The EPA believes that joint training and joint operations are essential before disasters occur. Its training serves the dual purpose of detecting environment crimes as well as preparing first responders for terrorist attacks using chemical, radiological and other environment contaminants.

11. Federal Bureau of Investigation (FBI). Presidential Decision Directive (PDD) 39, signed by President Clinton in 1995, defines the FBI's role in counter-terrorism. The Bureau is assigned roles in preparedness for, prevention of, and response to terrorist attacks. The FBI has the lead role for crisis management in these events. Leading the federal consequence management effort is the Federal Emergency Management Agency (FEMA).

The Bureau has a long history in counter-intelligence and has been working for well over a decade on terrorism. According to a recent *Washington Post* report, "in 1991, when the U.S. began its bombing campaign in Operation Desert Storm, Iraq's intelligence agencies attempted unsuccessfully to carry out terrorist bombing against U.S. embassies and other facilities,"[10] the FBI worked alongside the CIA and their peers in other nations to interdict the agents before they could damage worldwide U.S. owned facilities. The FBI has reduced its workload in some areas where heavier coverage could be provided by other federal law enforcement agencies. This has freed additional agents for assignment to the critical counter-terrorism function. Recently, the PATRIOT Act and other legislation have enabled the Bureau and federal intelligence agencies to share more information, more rapidly than in the past.

The Bureau has 56 field offices and over 400 resident agencies that have significant counterterrorism capabilities. For example, each field office has an Evidence Response Team, with law enforcement and forensic expertise, and a HAZMAT Response Team, with HAZMAT and explosive expertise which are available to deploy when and where needed. Similarly, each field office has an anti-terrorism task force, and Infoguard (computer intrusion program), key asset and weapons of mass destruction contingency planning coordinators. These special agents are available to advise and assist all law enforcement agencies, and calls are encouraged. The FBI also has an Indian Country Unit at its Washington, DC, headquarters. Its principal functions are providing training and support to law enforcement officers (FBI agents, BIA-OLES, and tribal officers) working in Indian Country. The unit is

United States Customs Service Recruitment and Information Booth.

headed by Supervisory Special Agent, Ernst H. Weyand, who attended the Summit. The FBI Indian Country Unit can be contacted at (202) 324-3802.

As part of the recent federal reorganization of law enforcement and security agencies, the National Infrastructure Protection Center, a cooperative effort among several federal agencies, is moving from FBI headquarters to the Department of Homeland Security.

12. Federal Emergency Management Agency (FEMA). FEMA has a long history of dealing with Indian nations and tribes on a government to government basis. However, depending on the focus and funding authority for certain programs, this is not always possible.

For example, the Fiscal Year (FY)–2002[11] funding for improvements in first responder capabilities is authorized through the Stafford Act which precludes direct government to government funding.[12] While Indian nations are not directly eligible for this funding they are urged to consult the October 1, 2002 edition of the Federal Register for grant guidelines. FEMA hopes that future legislation will permit direct funding to Indian nations and tribes.

Upgrading Emergency Operations Centers (EOCs) and updating emergency response plans are key FEMA goals; $56 million has been earmarked for upgrading EOCs. Those in the worse shape will be funded first and every EOC will receive a secure communications suite. However, the receipt of secure communications will require EOCs to increase the physical security afforded these sensitive communication centers. FY-2002 funding was provided to states on the basis of population alone. The more sparsely populated western states have objected to that formula believing that the perceived level of risk should be the principal determining factor for funding. FEMA expects that FY–2003 funding will be allocated with a certain base funding amount provided to each state, for example, $5 million. Funding over this base will be allocated based on population. Thus, without legislative intervention, tribal lands do not appear to be in line for direct funding of homeland security improvements until FY–2004, at the earliest.

13. Indian Health Service (IHS). Under the Federal Emergency Response Plan, which coordinates disaster response, the IHS supplies a broad variety of health and emergency medical services. The IHS is part of the Public Health Service which has 6,000 uniformed officers that are ready to deploy at any time, to any place, where they are required to alleviate public health emergencies. IHS is looking for tribes to develop Tribal control of the emergency medical response capabilities on tribal lands. It is also working to improve State/Tribal coordination.

United States Secret Service Uniform Division Officers keep a vigilant watch for well-qualified applicants.

Recently, States were asked to address the inclusion of tribes in their planning. Fourteen of the 35 states with Indian reservations did so. Of these 14, only one was willing to provide funds to tribes for staffing improvements in Indian response capabilities.

The IHS has no plans for mass inoculations of Native Americans against smallpox. Neither will there be mass inoculations in the rest of the nation. That decision was made based on a determination that the current vaccine has significant health risks. IHS expects significant reduction in the vaccine's side effects over the next twelve months. IHS has signed memoranda of understanding with Health Canada and its Mexican counterpart to provide support in times of national disaster. It is also looking at the role of the National Guard and Reserve Forces in bio-terrorism response in America.

14. Department of Veterans Affairs (VA). The VA's over riding mission is providing medical care to veterans. It also provides back-up support to both the Public Health Service (in the form of medical personnel) and to the Department of Defense (in the form of supplies and logistics). The VA's medical assets are

stationary fixed facilities. For that reason, victims will be brought to VA facilities rather than the VA going to disaster sites. Because the VA lacks trauma centers to treat violently caused wounds, patients normally will be treated at another medical facility first. Once their condition is stable they can be transported to a VA hospital.

Veterans Affairs is developing emergency response capabilities in the area of decontamination of medical facilities, personnel and patients. However, national authorities are redefining its precise role in the Federal Disaster Response Plan. As part of the National Disaster Management System, the Salt Lake City, Utah VA Hospital has signed cooperative agreements with 22 area hospitals that will provide additional bed space in emergencies. Each VA facility will have different capabilities. When making homeland security plans, the VA Office of Policy and Planning (Washington, DC) should be contacted to determine exactly what capabilities are available at local VA facilities. The Policy and Planning Office can be reached at: (202) 273-5033.

Needed Resources

1. **Funding.** Most Native American communities do not have adequate funding to protect the critical infrastructure located on Tribal Lands. Current funding for Tribal law enforcement and first responders lags well behind that for non-Tribal law enforcement and first responders. The result is that many Tribal law enforcement and first responder systems lack personnel. In addition, some of the personnel they do have lack training, education, certification, experience, and sufficient technical assistance. Many others experience burn-out resulting in low retention rates. Lack of funding has also left many Native American communities without Tribal fire departments and health services. With an influx in funding, many of the above obstacles to eliminating the vulnerabilities located on Tribal Lands can be overcome.

   Summit participants believe that tribes should receive base funding to achieve parity with non-Indian communities for law enforcement and first responder capabilities, plus additional funding for specific high-priority protection, and for response and recovery projects. They felt that funding tribes on a per capita basis will not produce sufficient security improvement. Instead, funding should be sufficient to bring tribes up to a national minimum standard of law enforcement and first responder manpower, equipment and training.

   Participants said it is also critical that federal agencies include Tribal Nations in law enforcement and first responder grant funding as they do State and local governments. They said, Tribal Nations should be included in the Department of Homeland Security grants for homeland security and the Department of Justice grants administered by the Justice Assistance Grants program, which includes the Byrne and Local Law Enforcement Block Grants programs. The Department of Justice, COPS Office grants program is an excellent example of a grants program that includes Tribal governments in the grant access language. Participants strongly supported the concept of a legislative change that would allow the Department of Homeland Security to directly fund tribes on a Government-to-Government basis.

In short, much vulnerability exists on Tribal lands because Tribal communities lack the resources to address these vulnerabilities. The lack of resources is a direct result of inadequate funding. Inadequate funding has created a lack of law enforcement and first responder personnel, and has also given rise to insufficient training of existing human capitol, as well as greatly reducing technical assistance and resources. As such, inadequate funding is a major roadblock to the elimination of vulnerabilities on Tribal lands.

2. **Training.** Native American communities need more training and specific guidance regarding their role in the National Homeland Security Strategy and Defense. The 2002 NNALEA Tribal Lands Homeland Security Summit was just a starting point for such training and guidance. Although, in 2003 NNALEA will include a tract on "Homeland Security" training at its national conference, many other training programs are needed. When assessing homeland security training needs, the following should be taken into consideration:

- Trainers and planners need to think outside the box, in order to prepare America for the next terrorist attack, not the last one.
- Communities need to receive specific training to clarify missions, develop a collaborative strategy, and to identify goals and objectives. In addition specific training is necessary to establish performance measures in preparation for attacks that utilize chemical, biological, radiological and other weapons of mass destruction.
- Decontamination procedures training needs to be conducted at the local level incorporating the tabletop exercise approach in the curriculum.
- Communities need to train and plan to respond to denial of service attacks.
- For a community homeland security plan, to be implemented successfully, it requires high-quality management training that is focused on key proven success factors. Some of these factors requiring specialized training include human capitol management and strategy, risk management, information technology management, strategic planning and many other critical management processes. These key success factors will vary from community to community as will specific community homeland security plans. Therefore, strong consideration needs to be given to using an academic training consortium specializing in Tribal law enforcement, first responder, and homeland Security training. The Academic Center for Excellence in Native American Law Enforcement Training is a NNALEA partnership with Fort Lewis College, East Central University of Oklahoma, the Federal Law Enforcement Training Center–Distance Learning Program, and the Boys & Girls Clubs of America. The partnership is dedicated to bringing quality law enforcement, first responder, and homeland security training to Tribal communities.

3. **Equipment and Technical Assistance.** Community homeland security plans vary greatly from one community to another. Specific national standards have not been established to indicate what specialized equipment and technical assistance a community needs to have to achieve an acceptable level of homeland security preparedness. Tribal

communication systems, as well as the equipment of Tribal law enforcement, first responders and fire departments generally lack parity with their non-Tribal counterparts. Therefore, most Tribal Nations need additional basic law enforcement and emergency response equipment and technical assistance.

Summit participants made the following comments regarding Tribal homeland security equipment and technical assistance:

Equipment:

- Many Tribal Nations have volunteer fire departments which must meet both their fire emergency and chemical emergency response calls. These departments are generally in need of a broad variety of equipment including, but not limited to, personal safety equipment, protective suits and respiratory equipment.
- Tribal lands generally are in need of basic communications equipment. Tribal communities' homeland security planning calls for a communication system that will enable integrated communications with and between on-reservation and off-reservation fire and police agencies, of which most Tribal communities need.
- Most Tribal Fire Departments need basic response and fire equipment, from hoses and nozzles to pump trucks.
- Tribal law enforcement, first responders, medical providers and incident clean-up teams need a complete range of emergency equipment from personnel protective gear to biohazard identification equipment and disposal devises.

Technical Assistance:

- Tribal Nations generally do not have large bureaucracies with embedded scientists/experts or university communities which can provide on-site technical assistance in the more sophisticated management, forensic, security and scientific skills needed to develop well-rounded tribal homeland security programs. Therefore, obtaining a means for the technical assistance and expertise necessary for Tribal communities' homeland security planning and program development is needed.
- Technical assistance needed by Tribal Nations can be provided through contract sources.
- On-site Tribal homeland security needs for specialized expertise can be provided by circuit-riding experts who can visit individual Tribal Nations and inter-Tribal organizations to assist in the development of homeland security capacity-building.
- Tribal Nations need contract resources familiar with Tribal governance and agencies to develop both written and electronic educational and program implementation resources for distribution to the community. The Academic Center for Excellence in Native American Law Enforcement Training is an excellent resource for these Tribal homeland security needs.

4. **Jurisdictional Cooperation and Clarification.** Providing homeland security and protecting critical infrastructure and assets on Tribal lands is complicated by crime and jurisdictional issues that frustrate law enforcement personnel, as well as the Tribal, state and federal judicial systems. Indian Country jurisdiction, law enforcement and first responder issues need to be clarified.

Within the context of Homeland security, the significance of Native American sovereignty lies in the manner in which the Department of Homeland Security should interact with Indian Nations. Indian leaders feel a deep sense of responsibility for the well being of members of their Nation. This is a cultural inheritance inseparable from being Indian.

NNALEA Summit Report
Page 22

Jurisdictional cooperation and clarification may, in part, be achieved by the following:

- Development of legislative language is needed that clarifies the right of Indian Nations to arrest, detain, and prosecute non-Native Americans committing crimes on Tribal reservations and trust areas.
- Uniform national standards are needed for law enforcement officer and first responder training and certification.
- States need facilitation and encouragement to enter into cross deputation agreements with Tribal Nations to facilitate the mutual sharing and support of peace officers, particularly in times of crises.
- Legislation with adequate funding is needed to bring Tribal courts, law enforcement, and first responders to parity with their non-tribal counterparts relative to pay, equipment, education, technical assistance, technology, and jurisdictional authority.
- Legislation is needed that gives clarification of the Government to Government relationship between Tribes and the Federal government on issues relating to the National Homeland Security Strategy and Defense.

SUMMIT GOALS
Goal 4: Identifying Mechanisms for Cooperation

As the Homeland Security strategy encompasses our entire country, cooperation between Native Americans and non-Native Americans is essential. As a means to promote cooperation, the attendees of the NNALEA Summit suggested that non-Native Americans gain a better understanding of Native Americans and their Tribes' sovereignty rights, while Native Americans gain a better understanding of the Federal Government and the roles of states and local governments.

Understanding Native Americans

Who are Native Americans?

Native Americans (often called American Indians) are Americans who trace their heritage to the original people of North America. Each tribe sets its own criteria for membership. There are 561 federally recognized tribes.[13] Native Americans have fought in every war in which the United States has been involved. No fewer than 16 Native Americans have been awarded the Medal of Honor, America's highest military decoration.[14]

Native Americans [are] 1.5 percent (4.1 million) of the U.S. population of 281.4 million,[15] which has grown 110 percent since the 1990 census, compared with 13 percent for America as a whole. Native Americans live in cities and towns throughout America in addition to the four percent of the American land designated as reservations and trust areas. Native Alaskan corporations own an additional 40+ million acres in Alaska.

How do Native Americans differ from the rest of America?

Native Americans are not a single group. Each tribe has its own unique governments whose goals, objectives, financial status and problems differ one from another. Some tribes are relatively affluent, others are very poor. Tribal members' goals, dreams, and aspirations also differ as do their living arrangements. Some Native Americans live on reservations and trust lands while others are integrated into America's neighborhoods.

According to the Census Bureau, Native Americans differ from the U.S. population generally by being younger, having higher fertility rates, being poorer, and being subject to more violent crime than any other U.S. minority group. Thirty-nine percent of the Native American population is under 20 years old with a median age of 26. The corresponding figures for the nation as a whole are 29 percent and a median age of 33, respectively.[16] Over the last decade the percentage of Americans claiming Native American ancestry has increased from 1 to 1.5 percent of the population.

Native Americans, as a group, have low incomes. The median family income is about $13,500 or 38 percent less than the median $35,335 of the average American family. Thirty-one percent of Indian families live below the poverty line compared to 13 percent of American families as a whole.[17] Within the Native American community, those who live on reservations and trust lands administered by the Bureau of Indian Affairs have the lowest incomes and a standard of living that would be unacceptable to most Americans. For example, the average per capita income for all Native Americans was $8,328. For Native Americans residing on reservations and trust

land that average was $4,478, varying from about $3,100 per person on the Pine Ridge (SD) and Tohono O'Odham (AZ) Reservations to $4,718 per person on the Blackfeet (MT) Reservation. These differences in wealth will require relatively higher federal homeland security funding for poorer tribes.

President Richard Nixon summarized the status of Native Americans as, " . . . the most deprived and most isolated minority group in our nation. On virtually every scale of measurement—employment, income, education, health—the condition of the Indian people ranks at the bottom."[18]

Where do Native Americans live?

About half of the Native American population live in neighborhoods throughout the United States, while the other half lives on reservations and trust lands that are administered by the Department of the Interior through its Bureau of Indian Affairs (BIA). Although there are 314 reservations and trust lands in the U.S., half the reservation population live on just 10 of these. They are: Navajo Reservation and Trust Lands (AZ, NM, UT); Pine Ridge (SD); Fort Apache (AZ); Tohono O'Odham (AZ); Gila River (AZ); Rosebud (SD); San Carlos (AZ); Zuni Pueblo (AZ-NM); Hopi (AZ); and Blackfeet (MT).

Housing is of much poorer quality on tribal lands than throughout the rest of America. Twenty-six percent of the housing in these communities lacks piped water, a toilet and a bathtub or shower. While most of the country is using the internet and preparing for high speed digital access, 23 percent of rural Native Americans lack basic telephone service.[19] In 1995, the Census Bureau concluded that American Indians living on Indian reservations "were as likely to lack complete plumbing facilities in 1990 as all U.S. households were *in the 1950's (sic).*"[20] (Italics are from the Census Report).

Understanding Tribal Sovereignty

Indian Tribes are Sovereign Nations

Sovereignty is an international concept that recognizes the power of a people to establish political structures to govern themselves. It means, according to Webster, "supreme and independent political authority."[21] Tribal sovereignty is the history and current practices that American Indian tribes have of managing their own affairs.

Native American mother and child from the Nez Perce Indian Reservation.

It is vital that both federal and state leaders understand the sovereignty inherently possessed by federally recognized Native American nations and tribes. It is unique in our Nation. Without understanding the Constitutional, treaty, statutory and judicial basis for this sovereignty, elected and appointed homeland security officials will be hard pressed to effectively communicate with or understand the tribal governments with which they must deal. Certainly, they risk being unable to harmoniously and effectively carry out their responsibilities.

All Americans learn that, under the Constitution of the United States, a federal relationship exists between the United States and state governments. The federal government is supreme and obtains its power from the consent of the citizens it governs.

Indian Nations "Higher Status" with the Federal Government

Indian tribes are the original Americans. They populated America well before European explorers and settlers arrived. **The Constitution recognizes Indian tribes as separate, distinct and unique governments.** Article 1, section 8, clause 3, authorizes Congress to regulate

commerce with "foreign nations, among the several states, and with the Indian tribes."

According to the court in McClanahan v. Arizona Tax Commission, "Indian tribes have inherent powers deriving from a sovereign status. Their claim to sovereignty long predates that of our own government."[22] Thus, the relationship between the U.S. government and Indian tribes is unique because Indian tribes derive their powers from their sovereign existence as well as through delegation of power from the federal government.[23] As the Ninth Circuit declared in 1965, "Indian tribes are, of course, not states; they have a status higher than those of states. They are subordinate and dependent nations, possessed of all powers as such, and limited only to the extent that they are expressly required to surrender their powers by the superior sovereign, the United States."[24]

Children embrace their Native heritage through tribal costume and dance.

Felix Cohen, wrote an extensive and authoritative tome entitled, *Handbook of Federal Indian Law* for the Department of the Interior. According to Cohen:

The most basic principles of Indian law supported by a host of decisions . . . is the principle that those powers which are lawfully vested in an Indian tribe are not, in general delegated powers granted by express acts of Congress, but rather inherent powers of a limited sovereignty that has never been extinguished. What are not expressly limited remains within the domain of tribal sovereignty *(emphasis in the original source)*.

The Constitution of the United States, 371 Nation-to-Nation treaties (between the federal government and Indian tribes), federal statutes, case law, executive orders and other administrative policies protect the government-to-government relationship between the federal government and federally recognized tribes. Cohen explains that, "Each Indian tribe begins its relationship with the federal government as a sovereign power, recognized as such in treaty and legislation. The powers of sovereignty have been limited from time to time by special treaties and laws."[25] Case law establishes that tribes reserve the rights they have never given away.

The Government-to-Government Relationship

Over the years, various Indian tribes (hereafter referred to as Indian Nations in recognition of their status as sovereigns with the right of self-determination and self regulation) entered into agreements with the federal government. Sometimes, these agreements limit some external powers of the Indian Nation, for example, its power to enter into treaties with foreign governments, in return for the U.S. government providing something to the Indian tribe. Examples include guarantees of protection, peace, recognition of borders, continued rights of self governance, land rights, etc.

The Chippewa and Sioux Nations of Minnesota, for example, were never conquered and yet entered into treaties of peace and protection with the United States. In Worchester v. Georgia, Chief Justice Marshall said,

" . . . settled doctrines of the law of nations is that a weaker power does not surrender its independence—its right to self government—by associating with the stronger and taking its protection. A weak state, in order to provide for its safety, may place itself under the protection of one more powerful, without stripping itself of the right of government and ceasing to be a state. Examples of this kind are not wanting in Europe. The Cherokee nation, then, is a distinct

community occupying its own territory, with boundaries accurately described, in which the laws of Georgia can have no right to enter, but with the assent of the Cherokees themselves, or in conformity with treaties, and with the acts of Congress. The whole intercourse between the United States and this nation is, by our Constitution and laws, vested in the government of the United States."[26]

Tribal sovereignty is more than of historical interest. Over several decades, the U.S. Supreme Court and lower federal courts have applied the principles of Indian sovereignty to determine: the authority of tribal courts, criminal jurisdiction, extradition, licensing, sovereign immunity and taxation. Tribal sovereignty, in short, means four things:

1. Tribes are sovereign nations possessing the right of self governance,
2. Native American tribes have a Government-to-Government relationship with the federal government,
3. Only Congress has the power to regulate Indian affairs and change agreements and the conditions affecting Native American nations, and
4. State governance within Indian Country is limited.

Presidential Support of Native American Self Determination

In 1970, President Richard Nixon recognized that past federal Indian policy vacillated between the two extremes of paternalism and forced termination of the federal trustee relationship with Native American Tribes. He felt that it," . . . must be the goal of any new policy toward the Indian people to strengthen the Indian's sense of autonomy without threatening his sense of community." He suggested, "a policy in which the federal government and the Indian community play complementary roles," and states that "Most importantly, we have turned from the question of whether the federal government has a responsibility to Indians to the question of how that responsibility can be furthered.[27]

Beginning with the administration of President Nixon, the federal policy toward tribes has been to support tribal sovereignty and tribal self determination. President George W. Bush has continued this time-honored policy.

Tribal Sovereignty and the Department of Homeland Security

Within the context of Homeland security, the significance of Native American sovereignty lies in the manner in which the Department of Homeland Security should interact with Indian Nations. Indian leaders feel a deep sense of responsibility for the well being of members of their Nations. This is a cultural inheritance inseparable from being Indian.

Presentation from Summit President Jim Wooten to Brad Buckles, Director of BATF.

Therefore, NNALEA recommends that the Department of Homeland Security open channels of communications directly with Native American nations. Through these channels, it must discuss how to improve homeland security on tribal lands. Successful application of this approach will result in producing seamless security at low cost. Both the Department of Homeland Security and

the Indian nations have the same goal—improved homeland security at reasonable cost. The Department's strategic leadership will be strengthened by receipt of the detailed knowledge of Indian lands and their vulnerability, possessed by the Indian Nations.

The alternative, attempting to communicate, fund or interact with Indian communities through states will take longer and possibly create unnecessary roadblocks, such as:

- ⇨ legal issues regarding lack of state authority on Tribal lands, and
- ⇨ insensitivity to the legal and cultural history of Indian sovereignty.

In sum, NNALEA advises that homeland security planning and funding not be passed through states to Indian nations, but be provided directly to Indian nations either individually or in regional consortiums or similar groupings. The Indian nations are eager to work with state and local governments to reduce duplication and expense and to provide America with seamless homeland security.

However, it will be difficult for Indian nations to work through these entities. Although this difference may appear small, it may be the difference between success and failure in providing effective homeland security for Native American communities.

Funding homeland security improvements in states but not on Indian lands is not a viable alternative to working with Indian nations for two reasons:

1. The potential of a catastrophic impact (beyond just the reservation) of successful attacks on vital targets on Tribal lands.
2. Every successful effort to harden sites outside Tribal lands will increase the vulnerabilities of people, assets and infrastructure on Tribal lands as they remain softer targets easier for terrorists to successfully attack.

SUMMIT GOALS
Goal 5: Defining Next Steps for Moving Forward

The final goal targeted and achieved by the attendees of the NNALEA Summit, was to determine the next steps for moving forward with homeland security on Tribal lands. The attendees made numerous recommendations, several of which are set forth below. In addition, this report concludes with a summary of NNALEA's Homeland Security Summit Assessment Model.

General Recommendations

For seamless communications between federal, state, and local governments when working with tribal governments on homeland security issues:

1. View Indian nations as separate entities because each is unique.
2. Communicate directly with Indian nations.
3. Provide funding directly to Indian nations.
4. Strengthen lines of communication between tribal governments and non-tribal emergency and law enforcement agencies.
5. Address liability and jurisdictional issues that limit the ability of state, local and Tribal law enforcement groups to work together.

Recommendations for the Department of Homeland Security:

1. Develop a comprehensive list of potential terrorist targets within the Tribal lands as well as the rest of the United States.
2. Establish a coordination unit within the Department to provide a single point of contact for the Indian Tribes. This unit should be the conduit for the distribution of the tribal share of homeland security funding directly to the Tribal governments involved. Such would also be in accordance with the principle of tribal self-governance.
3. Apportion homeland security funds based on the cost of reducing specific priority vulnerabilities, not solely on population or other criteria.
4. Develop a homeland security emergency communications system and frequency that all levels of government—federal, tribal, state, and local—have access to and which provides two-way communication of terrorist alerts, notification of natural and man made disasters, and relevant operational intelligence.
5. Encourage state and local governments to enter into mutual support agreements with tribal governments to share complimentary resources in times of crises.
6. Encourage state and local jurisdictions to establish agreements with tribal governments that cross deputize and provide certified Indian Police Officers equivalent status to other police officers.

Recommendations for the Department of Justice:

1. Develop legislative language that clarifies the right of Indian nations and tribes to arrest, detain, and prosecute non-Native Americans committing crimes on reservations and other Tribal lands.
2. Develop uniform national standards for law enforcement officer and first responder training and certification.

3. Encourage States to enter into agreements with Tribal governments to cross deputize and to facilitate the mutual sharing and support of peace officers, particularly in times of crises.

Recommendations for NNALEA:

1. Distribute and update the "NNALEA Homeland Security Assessment Model."
2. Assist Indian Tribes with the NNALEA homeland security assessment process.
3. Develop and provide tribal law enforcement and tribal first responder homeland security training.
4. Continue to provide a forum for the discussion of tribal homeland security.
5. Lead in the development of a strategic homeland security defense plan for Tribal lands.
6. Post links on the NNALEA website to pertinent homeland security websites.
7. Provide technical assistance to Indian Tribes relative to homeland security.
8. Continue to promote partnerships that facilitate Indian Tribes' role in the National Homeland Defense strategy.

Recommended Next Steps: Strategic Planning for Tribal and Non-Tribal Communities:

The National Homeland Security Strategic Plan needs to be flexible and fully implemented at all levels of government and the private sector. Development of the National Strategic Plan is an ongoing iterative process that requires a great deal of patience and hard work. Collaboration clarifies priorities, focus, funding levels, formulas and other key proven success factors. NNALEA recommends that communities mirror the evolving National Homeland Security Strategic Plan when developing their respective community homeland security strategic plan. The following examples will assist in the process:

1. The July 2002 National Homeland Security Strategic Plan is but a start. From its five-year perspective, the national annual plan is designed to incrementally improve homeland security. Planning extends to individual communities which can then develop their own five-year strategic plans. These plans incrementally improve local homeland security and defense by defining annual goals and objectives.
2. The National Homeland Security Strategic five-year Plan has been disseminated by the federal government to tribal, state and local governments. Likewise, communities can disseminate their respective five-year strategic plans to federal, state, and local governments, law enforcement, first responders, and citizens within their respective boundaries.
3. The National Homeland Security Strategic Plan should at a minimum be evaluated at a national level biannually through embedded accountability criteria. In addition, it is important for communities to embed similar accountability criteria into their respective homeland security strategic plan. These criteria will enable evaluators to regularly monitor and report the progress and compliance with the National Homeland Security Strategic Plan.
4. National accountability criteria data is collected through exercises, experiences, intelligence, and accomplishments. The data provides feedback enabling adjustment to the National Homeland Security Strategic Plan in a timely fashion. As milestones of the plan are achieved,

funding is freed to improve other vital needs. Similarly, communities with accountability criteria designed into their respective homeland security strategic plan will collect data through local exercises, experience, intelligence, and accomplishments. Thereby, enabling adjustments to the communities' homeland security plan in a timely manner, freeing funding for other vital needs.

5. During the five-year tenure of a National Homeland Security Strategic Plan, staff from all levels of government continuously monitor, review and evaluate the national plan. Based upon input from federal, Tribal, state, and local governments, agencies, the private sector, national and international intelligence sources, world events, and non-governmental organizations, the National five-year Strategic Plan continually evolves. The five-year tenure of a respective community homeland security strategic plan, will utilize national guidance along with grassroots input to develop and evolve their respective plan.

6. At the end of a five-year strategic plan, the process normally begins anew. However, a variety of national or world events may require that a national and/or community five-year homeland security strategic plan be extensively revised or replaced with a new strategic plan. This flexibility is crucial.

The NNALEA Homeland Security Improvement Model

The NNALEA Homeland Security Improvement Model was designed to assist communities in the development and improvement of their respective community homeland security strategic plan. The NNALEA model is flexible, adaptive, timely and reactive to the National Homeland Security Strategic Plan. As the national strategic plan evolves and changes based upon collaborative analysis and changing world events, the use of the NNALEA Homeland Security Improvement Model will empower a community to be in step with the National Homeland Security Strategic Plan and to fit seamlessly into the fabric of the National Homeland Security Strategy and Defense.

NNALEA Homeland Security Assessment Model

International and domestic terrorism is a part of life in 21st century America. As many of our Summit attendees pointed out, Native Americans are no strangers to terrorism. As one attendee stated, "Native Americans are experts on the impacts of losing the war for homeland security. We have a long history of military service to the United States in foreign wars. Our challenge now is at home, in our communities. To maintain our freedom and liberty, both the United States and our Indian Nations must remain open, but we must increase our preparations and vigilance."

We cannot provide, let alone afford, 100 percent protection for every possible terrorist target. Our challenge is to develop interconnected, reinforcing and complementary systems, both within and outside tribal lands that protect our communities and ensure that essential requirements and services are provided that avoid unnecessary duplication. This security model provides a process for enhancing emergency services and securing our communities while cooperating with local, state and federal governments, as together we strive to protect our Homeland.

NNALEA drafted this five-part "Homeland Security Assessment Model" to provide structure to the Summit and to provide Tribal leaders a beginning point from which security needs could be assessed and improvements made. Its ultimate purpose is to assist tribal leaders, emergency response planners, law enforcement officials, and owners and operators of likely targets in working together to provide safety and security for Tribal lands, and in turn our country as a whole. We believe that completion of an assessment, like this model, assists tribes and communities in taking stock of both their resources and needs. The assessment model will help simplify the process of requesting funding for specific improvements. It will also provide the information to strengthen the case for why specific efforts should be funded. The overall goal is to assist tribal governments in preventing terrorist attacks. Where that is impossible, the goal is to provide a method to reduce vulnerability, limit damage and speed recovery from successful attacks.

As discussed throughout the "Tribal Lands Homeland Security Summit," which refined this model, the evaluation process is simple in its construction, but complex in its details. Only by following a structure where we understand the threat and our vulnerabilities, assess and prioritize our risk, inventory our equipment and strengths, and seek cooperative agreements with others to share resources in emergencies, can we develop and price a list of the capabilities that are needed. This process leads to a prioritized list of necessary capabilities that is easily defended to federal and state officials seeking to best distribute homeland security funding.

I. Understanding the Threat[27]

What is homeland security?

Homeland security is a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur.

What is terrorism?

Terrorism is any premeditated, unlawful act, dangerous to human life or public welfare that is intended to intimidate or coerce civilian populations or governments. This covers kidnappings; hijackings; shootings; conventional

bombings; attacks involving chemical, biological, radiological, or nuclear weapons; cyber attacks and other forms of violence. Terrorists can be U.S. citizens or foreigners, acting alone, in concert with others, or on behalf of a hostile nation or group.

Who are potential terrorists? What are their motivations?[29]

Public statements and the philosophies expressed by terrorist organizations indicate that the key to understanding the terrorist mindset lies in the terrorists' feelings of exploitation and vulnerability. Generally, terrorists view themselves as oppressed people. Their violent activities appeal primarily to individuals and groups living on the economic and social margins of their societies. Terrorist leaders and followers alike share a sense that people from outside their immediate group have used unfair means to take what is rightfully theirs. They also appear to believe that non-violent means of redressing their grievances are not available to them or would be ineffective. Even though some terrorist leaders are well educated, they and members of their groups espouse a simplistic view of how society operates. To them, society is hopelessly corrupt and their sense of hopelessness turns into rage and hatred and motivates them to seek extreme remedies.

Based on their public statements, terrorists appear to use three psychological defense mechanisms to ward off their feelings of vulnerability and hopelessness. These are projection, rationalization and identification. Projection is attributing a person's feelings to someone else. Thus, terrorists divorce themselves from their own feelings of hatred and rage by ascribing them to their perceived enemies. They falsely believe that their perceived exploiters intend to destroy them. Thus, they believe that they must destroy their exploiters by any means available.

Rationalization allows terrorists to overcome feelings of hopelessness by creating an alternate view of reality that justifies direct violent action. This weltansuang or world view can be either religious or secular. For example, it can take the form of a unique religious interpretation of scripture that promises a return to a purer, holier state or admission to paradise. Alternatively, it can be based on a theory of economic materialism or ecological determinism that promises the creation of a Utopian state. In either case, the use of rationalization provides a goal that energizes terrorists repressing their feelings that life is hopeless.

Identification appears to be the cement that holds terrorist organizations together. All members share, and identify with, the belief that they are persecuted by others who are inherently evil. They also share a Utopian rationalization to justify their actions. Often they identify with symbolic figures, e.g. great religious or political leaders, who overcame persecution and triumphed by using the same rationalization they seek to apply.

The result is groups whose view of the world is markedly divorced from what most would recognize as reality. The leaders of such groups fabricate their world view to justify violent actions. Such leaders are often reclusive, narcissistic and schizoid. Their followers are often young, naive, dependent and eager to share the better life their leaders promise. In this process they accept the leader's view as their reality.

Domestic Terrorists—Within the United States, for example, there have been both left- and right-wing terrorist organizations. These domestic terrorists have tried to use violence against civilians to start a revolution and bring down the government.

Foreign Terrorists—On the international level, Al-Qaeda has developed a powerful clandestine network that has two goals: the removal of Western influence from the Middle East, and the eventual establishment of a fundamentalist Islamic world order.

To many of us, these goals may not be very realistic nor do they justify harming innocent civilians. However, terrorists believe they are battling injustice. Their goals, however unrealistic in the opinion of others, provide them with what they feel is a justification for extreme acts of political violence.

What are likely terrorist methods?

In order to achieve their goals, terrorists normally organize themselves into clandestine cells of a few members each. The cells are connected by a common ideology and by an elaborate, but well disguised, system of communication and finance. Often there are several levels of intermediaries between cells. This prevents members of different cells from knowing one another or knowing the location of other cells. The lack of direct communication between cells makes it very difficult for governments to locate and remove terrorist organizations from society and prevent terrorist attacks. To complicate matters, most terrorist cells are "asleep" most of the time. Their members hold jobs or are students in local communities. They do everything they can to blend into the population. It is only when they are activated by a more-or-less centralized command structure that these "sleeper cells" finalize and implement their violent agenda.

Terrorists will apply the full range of weapons available to them—knives, sharpened objects, guns, improvised explosive devices, shoulder-fired missiles, weapons of mass disruption, attacks on computer systems, and weapons of mass destruction such as chemical, biological and nuclear weapons. Few attacks will be one-on-one; most will be designed to produce mass casualties and carnage. While use of weapons of mass destruction is the goal of the sophisticated terrorist groups with foreign government backing and global reach, most attacks will be by more conventional means. For all its destruction, the attacks on the World Trade Center and Pentagon were conventional—a plane used as a flying bomb or missile.

First responder systems, communications, plans, equipment, training, and hospital support will support the recovery from any weapons producing mass casualties. They also can produce benefits, on a daily basis, in areas under served by the health care system.

What are likely effects?

By unexpectedly attacking civilians through seemingly random acts of extreme and dramatic violence, terrorists hope to use a combination of psychological and economic impacts to accomplish their political goals. Psychologically, terrorists want the target population to become preoccupied with grief and be overcome by the fear of future attacks. They desire the population to live in a state of continual post-traumatic stress, constantly feeling vulnerable, and eventually believing that the battle against terrorism is hopeless and never-ending. By attacking highly visible targets and receiving news media coverage, terrorists hope to multiply the effects of their attack throughout the population.

Terrorists seek to cause three types of economic damage:

1. The direct economic impact of their acts. It's difficult to estimate the economic impact of the attack on the World Trade Center and the Pentagon. There was a significant loss of human life and a clear disruption of business and government which is hard to quantify. However, the

damage to the buildings alone and the cost of cleanup has been estimated at more than $30 billion.

2. The cost of combating future terrorist acts. The Department of Homeland Security, for example, will likely have an annual budget in the tens of billions of dollars. Additional homeland security expenditures by other federal, state, tribal and local agencies and the expense of interdicting terrorists abroad will add to the costs included in the budget of the Department of Homeland Security.

3. The impact on the wider business and financial community. Feelings of vulnerability lead to a lack of confidence and willingness to take risks. These affect business purchases, stock markets and broad sectors of the international economy, leading to a general economic slowdown. The impact of the World Trade Center attack on the airline and travel industries is a powerful example of how fear can create an economic multiplier effect.

Terrorists hope that these combined psychological and financial impacts will exhaust the resources of their targets and lead them to recognize the terrorists, negotiate their demands or capitulate to those demands.

What will it take to secure our nation?

Terrorism can be effectively controlled and eventually defeated by a concerted national effort. The federal (executive, legislative and judicial branches) government, tribal governments, state and local governments, private business and industry, and the American people all have a role to play. The Department of Homeland Security is but a single player. Our country belongs to all of us. It will take each of us working together, helping one another and coordinating our efforts to protect our country at a cost we can afford.

The first step in fighting terrorism is to isolate the terrorist organization from community support. Governments must make it clear, through public statements and actions, that they are pursuing individuals planning and performing violent acts, not ethnic or religious groups or peaceful political organizations.

The second step is to develop cooperation between all levels of government, the private sector and citizens' organizations by implementing an economically feasible and prioritized system of homeland security. Terrorist cells can be activated at any time to attack targets, produce fear and draw the attention of the news media. Trying to protect all potential targets all the time would be prohibitively expensive and, ultimately, impossible. All levels of government must work together with private industry and citizens' groups to protect first those targets that would do the most damage to our people and the economic base, upon which our society depends.

The third step, occurring simultaneously with the first two, is to prevent terrorist attacks. Our best defense is to deter terrorists from attacking us. We seek to disrupt terrorist cells and larger organizations to keep them off balance, degrade their capabilities, and uncover and frustrate their plans. National and international law enforcement agencies, the courts, military, and intelligence organizations have the lead in this effort. They must pursue, arrest, interrogate, and incarcerate members of terrorist organizations. Their financial assets must be seized and communications and supplies disrupted.

Public vigilance and reporting of suspicious acts is an important multiplier for the efforts of these agencies. Muslim citizens, in whose communities some terrorists hide, need to support America by reporting their concerns. As President Bush has said, millions of pairs of eyes being more vigilant and aware as we

"We (Native Americans) have a long history of military service to the United States in foreign wars. Our challenge now is at home, in our communities. To maintain our freedom and liberty, both the United States and our Indian Nations must remain open, but we must increase our preparations and vigilance."

NNALEA Summit Report
Page 26

go about our daily lives inspire fear in terrorists and ultimately prevent attacks on our communities.

As one federal agent attending the Summit pointed out, "Terrorism is just another criminal enterprise. Although its members are dangerous, both fanatical and suicidal, it operates like any other criminal enterprise. It requires logistics and command and control to succeed. Terrorist operators-bombers, pilots or other front-line operatives, appear just before the act is to occur. Intercepting their communications and their logistic support equipment, and destroying their financing will disrupt their attacks and break their organization. Thus, it is a war that can be won even though it may take several years for intelligence and law enforcement to fully adapt and hone their techniques."

Reduce our vulnerability—by a systematic, comprehensive and strategic effort (between governments and the private sector) to identify and protect our critical infrastructure and key assets, detect terrorist threats and augment key assets. We must balance the benefits of reducing risks against both economic costs and infringements on individual liberty that might be entailed. These decisions must be made by politically accountable leaders exercising sound judgment with information provided by top-notch scientists, law enforcement and intelligence sources, medical experts, and engineers.

The SuAnne Big Crow Boys & Girls Club, located on the Pine Ridge Reservation in Pine Ridge, South Dakota.

Minimize damage—We must prepare to manage the consequences of successful terrorist attacks. This involves improving the system and preparing the individuals who will respond to acts of terror. These are police officers, firefighters, emergency medical providers, public works personnel, and emergency management officials and the equipment and systems they depend on.

Recover from attacks—We must build and maintain financial, legal and social systems to recover from acts of terrorism. This includes preparations to protect and restore institutions needed for economic growth and confidence, rebuild destroyed property, assist victims and their families, heal psychological wounds, demonstrate compassion and recognize we cannot always return to pre-attack status.

II. Defining Vulnerabilities

Organize the Process—What has already been done? Who are our local experts?

Involve all interested local parties and agencies, and include private corporations. Be inclusive, not exclusive; the more who become involved, the wider the pool of expertise and information available to assess vulnerabilities and plan actions.

Determine what the state and federal governments are doing, for example, what is the Federal Response Plan and how does it effect your jurisdiction? Is there a state Emergency Operations Plan? Does your state have an Emergency Coordination Center? Does your state have an Emergency Response Commission or agency? (The state of Alaska has a Terrorism Disaster Policy Cabinet that integrates all of these capabilities and more.)[30] Determine whether your jurisdiction has been included or overlooked. What vulnerabilities have already been identified? For example, The Federal Office of Homeland Security within the Executive Office of the President is building a nationwide listing of critical potential targets, and the State of Oklahoma is conducting a statewide threat and vulnerability assessment that will include a needs and capabilities assessment of law enforcement, fire service, public works, emergency medical services, public health systems and

agriculture. The state intends to assist urban and rural first responders in obtaining equipment and training through federal grants.[31]

Consider possible targets

Identify which facilities and locations would produce great loss of life or damage, symbolically attack the government or in other ways make news and gain attention for terrorists. Include:

Commercial Activities

- banks
- communications facilities and towers
- gasoline stations
- natural gas works and major users
- hazardous material storage facilities
- hospitals
- major industrial users of water/potential polluters (paper mills, linoleum factories)
- manufacturing industries (type, location)
- reservoirs and water treatment facilities
- processing industries (types and location)
- retail weapons sales, storage facilities, ammunition caches, dynamite sellers and users
- sports stadiums and facilities

Energy Infrastructure

- dams and hydroelectric power plants
- gas and oil pipelines
- coal, nuclear, solar power generating plants, distribution systems, grids
- power lines
- gasoline, natural gas, oil storage facilities and tank farms

Government Building and Facilities

- archives—public, semipublic, ecclesiastical, historical
- historic monuments and sites
- military armories, equipment facilities, reserve centers
- municipal water systems, supplies, filtration plants
- post offices
- public works and utilities plants, line systems, nets and connecting grids
- radioactive waste, garbage and refuse disposal system
- sewage collection systems and disposal plants
- schools
- storm drainage systems
- telephone exchanges, long-line systems and connecting grids
- international/intercontinental wire and submarine cables

Population Centers

- casinos
- community centers, churches (particularly of minority religions)
- convention centers
- tourist attractions

Transportation Infrastructure

- airports and air fields—location size, runway length and capacities of all
- bridges and overpasses
- harbors and ports, port services and repair facilities

- railroads—locations of switch yards, major terminals, tunnels

Utilities

- power sources, transmission facilities, grids
- radio and TV transmitting stations (number, type, and location), channels, frequencies, trunk lines
- water control and supply
- sewage and waste disposal systems

Inventory and Assess Potential Targets

As targets are identified, the inventory should include information on: what the target is, what its vulnerabilities might be, its location with map references, grid coordinates, or latitude and longitude, what environmental hazards does it represent, what is its size, who owns it, who is the security point of contact, how can they be contacted (i.e. telephone, fax and pager numbers, mailing and e-mail addresses). In addition:

- Assess the potential target by physical visits that catalog vulnerabilities (private facilities may have completed such an assessment)
- Determine causes of the vulnerability, the potential effects exploiting the vulnerability, and any low or no cost "fixes" that might improve its security
- Develop simple emergency scenarios—Conventional attacks (explosives, fire), cyber attacks, biological, and chemical attacks (these will be used in making risk assessments as well as in exercises to test actual responses). As emergency response activities mature, these scenarios can be increased in complexity and coverage area to test inter-jurisdictional communication, coordination and cooperation.

Assess Vulnerabilities and Risks[32]

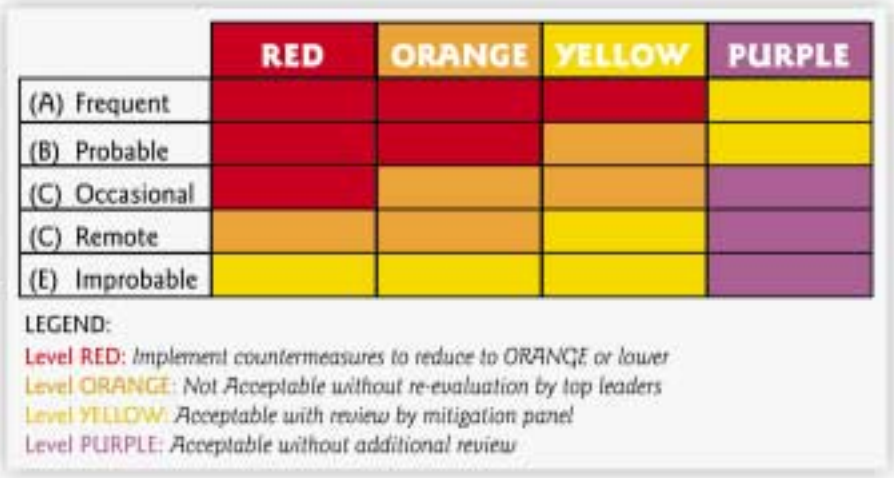
Determine potential severity and likelihood of damage or attacks. Use a Risk Assessment matrix to gauge the severity of consequence against the probability of attack to help prioritize the most significant vulnerabilities for remediation.

Develop Severity Measures, such as:

- **Severity Level RED—**Serious loss of life, casualties beyond ability of regional hospital system to cope; loss of critical asset or function; significant impairment of health and safety over a wide area.
- **Severity Level ORANGE—**Loss of life in a limited area; large number of hospitalizations within capability of tribal/local/regional government; loss of equipment, capacity or facilities requiring weeks or months to repair or replace; significant disruption to living conditions and commerce in a substantial area.
- **Severity Level YELLOW—**loss of life or severe injury to (insert number) or fewer people; deaths and injuries can be handled locally without straining facilities; limited or minor systems disruptions of fewer than 72 hours; no substantial danger to most of population
- **Severity Level PURPLE—**no loss of life; few serious injuries; no asset loss or system disruption for more than 24 hours; damage covers a small and easily controlled area

Develop Probability Categories, such as:

- **Frequent**—Possibility of repeated incidents
- **Probable**—possibility of isolated incidents
- **Occasional**—Possibility of occurring sometime
- **Remote**—not likely to occur
- **Improbable**—practically impossible



	RED	ORANGE	YELLOW	PURPLE
(A) Frequent				
(B) Probable				
(C) Occasional				
(C) Remote				
(E) Improbable				

LEGEND:
Level RED: *Implement countermeasures to reduce to ORANGE or lower*
Level ORANGE: *Not Acceptable without re-evaluation by top leaders*
Level YELLOW: *Acceptable with review by mitigation panel*
Level PURPLE: *Acceptable without additional review*

Analyze Counter Measures, Costs, and Technical Tradeoffs

This analysis works best when the team has a variety of skills represented (for example, a team might consist of an engineer, analyst, law enforcement officer or security specialist, local political official, business leader, health care professional, etc.)

- Develop solutions to reduce identified vulnerabilities.
- Determine costs (money, manpower, equipment).
- Decide to accept risk, eliminate it, or control it.
- Prioritize efforts (highest impact efforts first)—For example, the state of Alaska recognizes that the immediate threat of the terrorist use of nuclear and radiological devices is lower than the threat of the use of chemical, biological, explosive and incendiary devices. Thus it has prioritized its financial resources to upgrade its response abilities to reduce these dangers first.[33]

III. Identifying Resources—Available and Needed

Resources probably available include:

- maps of the area with key facilities noted
- aerial photography—available on the U.S. Geological survey website
- completed civil defense plans

Discuss planning and resources with, as many key officials and leaders as possible, including:

- local police and fire departments and those in adjacent localities; explore possibility of mutual support agreements
- utility owners (water, electricity, gas) including their security plans
- public work offices
- public sanitation officials
- local FEMA representative
- hospitals, emergency care and emergency response personnel
- school officials
- church officials and clergy

- state homeland security officials
- officials at local armories or military reserve centers

Calculate the shortfall, if any, between what is available and what is needed. Develop a list that matches the vulnerable target and proposed method for reducing its vulnerability with the resources that are needed, but unavailable. Ensure these resources are defined in detail, e.g., type radio or response vehicle needed and priced. By preparing this prioritized list, funding sources can more readily understand the improvements expected for the funds expended. Anticipate that, for example, federal agencies may be unwilling or unable to fund the tribe's highest priority need. Your list will facilitate obtaining funding for other needs, which may free tribal resources for its higher priority project.

IV: Identifying Mechanisms for and Roadblocks to Cooperation

The presence of tribal and non-tribal lands within a state presents many jurisdictional concerns and communication challenges to the law enforcement community. To address these concerns and maximize law enforcement resources, cross-deputization agreements should be considered between tribal governments, the Bureau of Indian Affairs, and local city/county governments. Cross-deputization agreements permit the signatories to commission or deputize a law enforcement officer of another signatory, thereby granting them the same law enforcement authority as officers of the commissioning department or agency. This has been especially successful in Oklahoma where its Indian Affairs Commission has facilitated 89 separate cross-deputization agreements since 1992. According to the Commission, which celebrated its 35th anniversary in May 2002, "the agreements have been instrumental in increasing law enforcement protection, especially in rural areas of Oklahoma."[34]

Other entities to consider include:

- Task Forces and Working Groups to facilitate emergency planning and coordination
- Public health entities
- County-wide or regional disaster planning task forces (training, assessments, exercises, emergency resources)
- Emergency response teams

V. Future Steps

- Collect information on federal and state programs, grants and funding sources.
- Involve as many departments and community members as possible.
- Determine how volunteer efforts can relieve first line responders from administrative tasks.
- Establish relationships with key federal and state homeland security officials.
- Develop a plan for what you need with justification and costs; include efforts to obtain the capabilities elsewhere or why that is impractical.
- Review and critique plan and revise where necessary.
- Are there mechanisms for resources sharing, including: Cooperative Agreements? Joint Plans? Joint Exercises?
- Have officials review in light of budgetary realities.
- Develop grant applications and approach federal and state funding sources.

⇨ Conduct exercises, critique exercises; identify weaknesses and prioritize fixes.

Conferees considered the need to establish personal relationships between Indian officials and federal, state, and local homeland security

Smith & Wesson representatives displays modern weaponry to conference participants.

officials, emergency planners, law enforcement, fire, public utility, corporate safety and security officials and others in key leadership positions, as vital. One conferee advised the Indian Nations not to wait to be invited. Show up at, for example, emergency planning meetings and ask how Indian Tribes are included in the plans being formed.

At the Summit, there was a general sense that since the 9-11 attacks, Americans have become closer and more willing to work together. This is a theme echoed throughout the President's Homeland Security Strategy. All levels of government must work together to provide complementary capabilities to thwart, respond to and recover from terrorist attacks. Cooperative efforts are all the nation can afford as it solves other problems such as Social Security and Medicare financing while fighting international terrorism, educating our youth, and maintaining other programs of national importance.

Address the Need for Accountability

It is undeniable that even the most prosperous tribes will require some public funding to improve their security, response and recovery capabilities. Whenever public monies are used, those spending them must ensure that they are properly used and accounted for. Determine early, how funds will be accounted for and who will audit the spending to ensure public monies are not mismanaged, wasted or misdirected.

⇨ Decide on evaluation criteria (what things will you measure?)

⇨ Determine how you will measure where you are now?

⇨ Determine how to measure progress or success against your baseline?

⇨ Devise a system to match costs to your measures of success.

⇨ Collect data on those measures to match level of success, level of efforts with costs.

DEFINITIONS

Indian Country

Land that is either:

(1) within a reservation,

(2) within a dependent Indian community, or

(3) on a tribal allotment.

Note: Tomas B. Heffelfinger, U. S. Attorney, Minnesota, to SCIA testimony 07/11/2002.

Tribal Lands

The term "Indian Lands" means all lands where Indian tribes or tribal members retain rights through federal statue, federally-recognized Indian treaty, federal executive order or judgments pronounced by federal courts of law. This includes lands with the limits of any Indian reservation under the jurisdiction of the United States, notwithstanding the issuance of any patent, and including rights-of-way running through the reservation; all dependent Indian communities within or without the limits of a state; all Indian allotments, the Indian titles to which have not been extinguished, including rights-of-way running through the same; all lands owned by federally-recognized tribes in Alaska or Alaska Native Corporations established under the Alaska Native Claims Settlement Act; all Indian lands held in trust or restricted status by the United States for member of a federally-recognized Indian tribe; and all lands where federally-recognized tribes have treaty rights to hunt, gather, fish or perform other traditional Indian activities.

Note: Dr. Martin Topper—email 2/18/2003

Indian Tribe

"Indian Tribe" means any Indian tribe, band, nation, or other organized group or community, including any Alaska Native village as defined in or established pursuant to the Alaska Native Claims Settlement Act (85 Stat. 688) [43 U. S. C. A. & 1601 et seq.], which is recognized as eligible for the special programs and services provided by the United States to Indians because of their status as Indians.

Explanation: This definition is the same definition used in the Indian Self Determination and Education Assistance Act, 25 U. S. C. & 450b, without the reference to regional or Village Corporation. The reference to the regional and village corporations was deleted because the activities in the proposed homeland security reorganization are government functions that are performed by the Alaska Native villages.

ENDNOTES

[1] NCAI Executive Director Jaequeline Johnson was the Keynote Speaker for the National Native American Law Enforcement Association's 10th Annual National Training Conference in Reno, Nevada, October 22, 2002.

[2] Gary L. Edwards. Testimony before the U.S. Senate Committee for Indian Affairs. February 26, 2003. Readers are invited to read the full text of Mr. Edwards' remarks on the NNALEA website at *http://www.nnalea.org/PDF/Gary's%20Testimony.pdf*.

[3] Readers are invited to read the full text of Chairman Campbell remarks. They are available on the website of the Senate Committee on Indian Affairs at: *http://www.indian.senate.gov/CampbellSecurity.pdf*.

[4] The Al Qaeda main mission, according to its military training manual, is "the overthrow of the godless regimes and their replacement with an Islamic regime." The targets cited above are taken from the top 8 targets listed in the translated military manual. (page UK/BM-12). The manual was publicly released during the embassy bombing trial in New York City as Government Exhibit 1677-T.

[5] Readers are invited to read the full text of Chairman Campbell remarks. They are available on the website of the Senate Committee on Indian Affairs at: *http://www.indian.senate.gov/CampbellSecurity.pdf*.

[6] These data were compiled from various infrastructure websites. Please contact NNALEA at *www.info@nnalea.org* for specific information on this material.

[7] These data were compiled from various infrastructure websites. Please contact NNALEA at *www.info@nnalea.org* for specific information on this material.

[8] The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, p. 19. You may download this document from the White House website at *http://www.whitehouse.gov/pcipb/physical.html*.

[9] The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, p. 19. You may download this document from the White House website at *http://www.whitehouse.gov/pcipb/physical.html*.

[10] Walter Pincus, "CIA, Allies Tracking Iraqi Agents—Agencies launch efforts to foil terrorist attacks," in The Washington Post, February 4, 2003, p. A17.

[11] The federal fiscal year is the basis for congressional appropriations, running from October 1st to September 30th. Thus Fiscal Year 2002 is the period October 1, 2001 to September 30, 2002.

[12] The Robert T. Stafford Disaster Assistance and Emergency Relief Act, 42 U.S.C. 5121 et seq., PL 93-288, defines "any Indian tribe or authorized tribal organization, or Alaska Native village or organization." 42 U.S.C. 5122 (6). Under this definition Indian Nations are not eligible for direct funding. Any funding they receive must come through a state. Thus tribes are given a federal status similar to that of a subordinate local government (town, county, village etc.). Besides the sovereignty issue, previously discussed, there are two other problems with tribes receiving funding this way, 1) several reservation cross state boundaries, for example the Navajo reservation crosses four states, which state, if any should provide funding to the Navajo? and 2) since states have no authority on Indian reservations, many governing authorities look upon Indian reservations as a federal responsibility. As a result, they do not allocate any funding to the tribes. Creating a vicious circle in which neither federal nor state governments are including Indian lands in their programs and funding decisions.

[13] Cheryl Simrell King and Casey Kanzler, The Impact of tribal Gaming on Indians, Tribes and Their Surrounding Communities in the State of Washington, 2002, p.2. An Indian Tribes is a group of people with a shared culture, history, and tribal government. To be federally recognized, the tribe must have a continuing relationship with the federal government. This relationship must have been created through a treaty, executive order, or legislation.

[14] COL Jerome T. Moriarty, unpublished, draft paper on Native American Medal of Honor Recipients. Twentieth Century recipients are listed on the Naval Historical Center website at *http://history.navy.mil/faqs/faq61-3.htm*.

[15] Stella U. Ogunwole, The American Indian and Alaska Native Population, Census 2000 Brief C2KBR/01-15, The Department of Commerce, U.S. Census Bureau, Issued February 2002, p.3.

(endnotes, continued)

[16] These data are taken from, The American Indian, Eskimo and Aleut Population, by Edna L. Paisano, U.S. Department of Commerce, Economics and Statistics Administration, U.S. Bureau of the Census. This document is accessible via the Internet at: *http://www.census.gov/population/www/pop-profile/amerind.html.*

[17] In 1989 the poverty threshold for a family of four was $12,674, the same, in 1989 dollars, as it was a decade before in 1979. Ibid., pp. 1-3.

[18] President Richard M. Nixon, Special Message on Indian Affairs, (to the Congress of the United States), July 8, 1970.

[19] Tex Hall, "The State of Indian Nations Today—Mapping a Course for the Next Seven Generations," a state of Native America address by the President of the National Congress of American Indians, January 31, 2003.

[20] Department of Commerce, Economics and Statistics Administration, Bureau of the Census, Statistical Brief: Housing on American Indians on Reservations—Plumbing, SB/95-9, Issued April 1995. Once again data show wide variations, between reservations, in the percentage of homes lacking complete plumbing. While the average is 20.2 percent, the percentage ranges from .5 percent on the Colville Reservation in WA to 49.1 percent on the Nez Perce Reservation in ID, and 46.7 percent on the Hopi Reservation and Trust Lands in AZ. (See the 3rd section of the table on page 2).

[21] Jean L. Mckechnie, Webster's New Twentieth Century Dictionary of the English Language (Unabridged), Second Edition, Simon and Shuster, New York, NY, 1983, p. 1736.

[22] *McClanahan v. Arizona Tax Commission*, 411 U.S. 164, 36 L.Ed. 2d 129 (1973).

[23] Chief Justice John Marshall was among the first jurists to clarify the status of Indian nations saying," The very term 'nation,' so generally applied to them (Indians) means 'a people distinct from others.' The Constitution, by declaring treaties already made, as well as those to be made as the supreme law of the land, has adopted and sanctioned the previous treaties with the Indian nations, and consequently admits their rank among those powers that are capable of making treaties. The words 'treaty' and 'nation' are words of our own language, selected in our diplomatic and legislative proceedings by ourselves, and have a definite and well-understood meaning. We have applied them to the other nations of the earth. They are applied to all in the same sense." (Quoted in Levanthal)

[24] *Colliflower v. Garland*, 342 F 2d. 369 (1965).

[25] Felix Cohen, Handbook of Federal Indian Law, Department of the Interior, 1942, p.123, quoted in Levanthal.

[26] *Worchester v. Georgia*, 6 Pet. 515 (1832).

[27] President Richard M. Nixon, Public Papers of the Presidents of the United States: Richard Nixon, 1970, pp. 564-567, 576.

[28] These definitions and goals are taken from the National Strategy for Homeland Security, Executive Office of the President, Office of Homeland Security, July 16, 2002. (This document is reproduced in its entirety and in executive summary format on the CD-ROM accompanying these Proccedings.)

[29] This section is extracted from a NNALEA copyrighted paper, "The Terrorist Mindset," by Dr. Martin D. Topper. A longtime NNALEA member, Dr. Topper is Co-Director of the Indian Country Homeland Security Summit. Dr. Topper is employed by the Office of Criminal Enforcement, Forensics and Training, of the Environmental Protection Agency. The opinions Dr. Topper expresses in this paper are his own and do not reflect the official position of any government agency.

[30] Maj. Gen. Phillip Oates, Adjutant General and Commissioner, Department of Military and Veterans Affairs, STATE OF ALASKA TERRORISM DISASTER POLICY CABINET: Executive Summary and Financial Information, November 12, 2001.

[31] Executive Office of the President, Office of Homeland Security. State and Local Actions for Homeland Security, July 2002, p.83.

[32] The NNALEA would like to acknowledge its debt to the Exxon Corporation, the United States Secret Service and United States Army, and its security and civil affairs doctrine for the ideas we have incorporated into this risk assessment process.

[33] Oates, p.4.

[34] For more information consult the web site of the Oklahoma Indian Affairs Commission at *http://www.oiac.state.ok.us/cca.html*

NATIONAL HOMELAND SECURITY STRATEGY OUTLINE AND OBJECTIVES

The primary result of this nation's search for answers and ways to reduce the terrorist threat was the formulation of the National Homeland Security Strategy, which sets forth three strategic objectives:

1. Prevent terrorist attacks within our homeland;
2. Reduce our Homeland's vulnerability to terrorism; and
3. Minimize the damage and recover from attacks that do occur.

These objectives are to be achieved in six initial areas, as defined by the Office of Homeland Security, namely:

1. Intelligence and warning—to detect terrorism before it manifests itself in an attack:
   a. Build new capabilities through the Information Analysis and Infrastructure Protection Division;
   b. Implement the Homeland Security Advisory System; and
   c. Apply dual-use analysis to prevent attacks.
2. Domestic counter-terrorism:
   a. Improve intergovernmental law enforcement coordination; and
   b. Track foreign terrorists and bring them to justice.
3. Border and transportation security.
4. Critical infrastructure protection
   a. Unify America's infrastructure protection effort;
   b. Build and maintain a complete and accurate assessment of America's critical infrastructures and key assets;
   c. Create effective partnerships with tribal, state and local government and the private sector;
   d. Develop a National Infrastructure protection plan; and
   e. Guard America's key assets and infrastructure against "inside" threats.
5. Catastrophic terrorism defense.
6. Emergency preparedness and response
   a. Create a national incident management system,
   b. Improve tactical counter-terrorist capabilities,
   c. Enable seamless communication among all responders,
   d. Prepare for NBC contamination,
   e. Plan for military support to civil authorities,
   f. Build the Citizen Corps,
   g. Build a training and evaluation system, and
   h. Enhance the victim support system.

NATIONAL NATIVE AMERICAN LAW ENFORCEMENT ASSOCIATION
Unity
Strength
Courage

GENERAL RECOMMENDATIONS OF THE SUMMIT ATTENDEES

For seamless communications between federal, state, and local governments when working with tribal governments on homeland security issues:

1. View Indian nations as separate entities because each is unique.
2. Communicate directly with Indian nations.
3. Provide funding directly to Indian nations.
4. Strengthen lines of communication between tribal governments and non-tribal emergency and law enforcement agencies.
5. Address liability and jurisdictional issues that limit the ability of state, local and tribal law enforcement groups to work together.

Recommendations for the Department of Homeland Security:

1. Develop a comprehensive list of potential terrorist targets within the tribal lands as well as the rest of the United States.
2. Establish a coordination unit within the Department to provide a single point of contact for the Indian tribes. This unit should be the conduit for the distribution of the tribal share of homeland security funding directly to the tribal governments involved. Such would also be in accordance with the principle of tribal self-governance.
3. Apportion homeland security funds based on the cost of reducing specific priority vulnerabilities, not solely on population or other criteria.
4. Develop a homeland security emergency communications system and frequency that all levels of government—federal, tribal, state, and local—have access to and which provides two-way communication of terrorist alerts, notification of natural and man made disasters, and relevant operational intelligence.
5. Encourage state and local governments to enter into mutual support agreements with tribal governments to share complimentary resources in times of crises.
6. Encourage state and local jurisdictions to establish agreements with tribal governments that cross deputize and provide certified Indian Police Officers equivalent status to other police officers.

(recommendations, continued)

Recommendations for the Department of Justice:

1. Develop legislative language that clarifies the right of Indian nations and tribes to arrest, detain, and prosecute non-Native Americans committing crimes on reservations and other Tribal Lands.
2. Develop uniform national standards for law enforcement officer and first responder training and certification.
3. Encourage States to enter into agreements with tribal governments to cross deputize and to facilitate the mutual sharing and support of peace officers, particularly in times of crises.

Recommendations for NNALEA:

1. Distribute and update the "NNALEA Homeland Security Assessment Model."
2. Assist Indian tribes with the NNALEA homeland security assessment process.
3. Develop and provide tribal law enforcement and tribal first responder homeland security training.
4. Continue to provide a forum for the discussion of tribal homeland security.
5. Lead in the development of a strategic homeland security defense plan for Tribal Lands.
6. Post links on the NNALEA website to pertinent homeland security websites.
7. Provide technical assistance to Indian tribes relative to homeland security.
8. Continue to promote partnerships that facilitate Indian tribes' role in the national homeland defense strategy.

National Native American Law Enforcement Association Homeland Security Pre-Assessment Meeting Outline For Tribal Nations and All Communities

This outline is based on the model used at the NNALEA Homeland Security Summit. It also can be used as a starting point for initial meetings of community leaders on local homeland security.

Purpose:

To help tribal, federal, state, local and private industry representatives develop a fundamental understanding of the potential threat to homeland security from domestic and foreign terrorist activities and to promote a cooperative effort to address that threat.

Goals:

1. Understand the threat
2. Define the vulnerabilities
3. Identify the resources, both available and needed
4. Identify mechanisms for cooperation
5. Define further steps

Format:

The format is a facilitated discussion between all representatives of tribal, federal, state, local and private industry organizations. Each block is somewhat different in format, depending upon the nature of its subject matter. Each block builds on information developed from the previous blocks to develop a "broad brush" understanding of the issues surrounding homeland security in a specific community or jurisdiction. Two facilitators work in tandem, and a recorder uses an easel to emphasize major points. A discussion leader works to keep the process moving forward.

Blocks

Block 1

Overview: "Terror and Homeland Security"

This block begins with an introduction by the leader, who welcomes participants to the and presents an overview of the meeting and its goals. The block continues with a presentation on terrorism and homeland security, which sets the tone for the working session. The presentation will discuss the nature of the terrorist threat, both foreign and domestic, and describe what the Nation is doing to meet that threat. The presentation will be followed by a brief question and answer period.

Block 2:

"Vulnerabilities and Impacts"

This block is an audience participation facilitated discussion. The facilitators use the following questions to generate discussion from the floor (other questions may be added):

- Who might initiate a terrorist incident in our area? Foreign? Domestic?
- What would their motives be?
- What might they target? Casinos? Energy infrastructure? Information Infrastructure? Business enterprises? Government facilities?
- What would they gain from attacking these various facilities?
- Do you have these facilities on your lands?

The block ends with the facilitators summarizing and identifying the vulnerabilities.

(outline, continued)

Block 3:

"Addressing Identified Vulnerabilities"

This block is an audience participation facilitated discussion. The facilitators use the following questions to generate discussion from the floor (other questions may be added later): For each vulnerability identified in the previous section, the following questions should be asked:

- If terrorists detonate a bomb or take other violent action at a facility (tourist attraction, power line) in our jurisdiction, who would respond?
- What are the differences between our jurisdiction and surrounding areas?
- What types of response plans do we have in place?
- Are there plans in place to identify threats and prevent attacks before they occur?

The block ends with the facilitators summarizing the complexity of addressing the vulnerabilities and stressing the importance of jurisdiction-specific planning and prevention.

Block 4:

"Resources"

This block is an audience participation facilitated discussion focused on resources. The facilitators will use the following questions to generate discussion (other questions may be added later).

- What types of resources are available to implement the plans described in Block 4?
- Are these plans and resources adequate to respond to the types of homeland security vulnerabilities defined in previous blocks? If not, what's needed?
- Are the plans and resources adequate to identify and prevent terrorist activities? If not what's needed?

The block ends with the facilitators summarizing the strengths and potential weaknesses of homeland security preparedness in the jurisdiction or community being evaluated.

Block 5:

"Cooperation: Federal Level"

This block involves a panel presentation and a facilitated discussion from the audience. The panel will be composed of representatives from invited federal agencies including, but not limited, to:

- Office of Homeland Security
- U.S. Secret Service
- FBI
- ATF
- DEA
- EPA
- FEMA
- BLM
- Customs Service
- Border Patrol
- VA

Each panelist will be introduced by the facilitators and asked several questions:

- What is the role of your agency in responding to and preventing terrorist incidents?
- How can that role assist our community/ jurisdiction in their homeland security preparedness efforts?

(outline, continued)

- What cooperative efforts do you currently have in place with our community/ jurisdiction?
- What area of cooperation needs to be developed?

At the conclusion of the questioning by the facilitators, the floor is opened for further questions from the participants in the audience. The block ends with the facilitators summarizing the various types of cooperation that have been established between the federal agencies and the community/jurisdiction under consideration, and defining areas that may be in need of further development.

Block 6:

"Cooperation: State/Local/Private Sector"

This block involves a panel presentation and a facilitated discussion from the audience. The panel is composed of representatives from states, localities and private sector companies that do business in the community/ jurisdiction under consideration. Each panelist is introduced by the facilitators and asked several questions.

- What is the role of your organization in responding to and preventing terrorist incidents?
- How does that role relate to the homeland security issues faced by the community/jurisdiction under consideration?
- What types of cooperative relationships do you have in place with our community /jurisdiction at the present time?
- What areas of cooperation need to be developed?

At the conclusion of the questioning by the facilitators, the floor is opened for further questions from the participants in the audience. The block ends with the facilitators summarizing the various types of cooperation that have been established between the federal agencies and the community/jurisdiction under consideration, and defining areas that may be in need of further development.

Block 7:

"What Have We Learned and How Can We Apply It?"

This block involves a review by the facilitators. They summarize what has been learned in each block and identify the strengths and weaknesses of the overall status of homeland security preparedness in the community/ jurisdiction under consideration. The audience is asked to provide input on this summarization. The facilitators work with the audience to build a consensus view of the vulnerabilities created by this threat, the level of local community/jurisdiction planning and preparedness, the existing resources, the level of cooperation on all levels of the public and private sector, and the need for the development of future resources and cooperative efforts. The facilitators then help the community/ jurisdiction develop an action plan for applying what has been learned and initiating the further development of the community/jurisdiction's homeland security system.

Block 8:

"Begin the NNALEA step by step Homeland Security Assessment Model"

This block ends the pre-assessment meeting phase. Apply the action plan developed in Block 7 above to the "Homeland Security Assessment Model" described on pages 28 through 36 of the "Tribal Lands Homeland Security Report."

NATIONAL NATIVE AMERICAN LAW ENFORCEMENT ASSOCIATION
Unity
Strength
Courage

Indian Country Border Security And Tribal Interoperability Pilot Program

(TBS PILOT PROGRAM)

The Importance Of Tribes At The Frontlines Of Border And Homeland Security

Submitted By:
The National Native American Law Enforcement Association
The National Congress of American Indians

Final Report
March 31, 2006

INDIAN COUNTRY BORDER SECURITY AND TRIBAL INTEROPERABILITY PILOT PROGRAM
(TBS PILOT PROGRAM)

THE IMPORTANCE OF TRIBES AT THE FRONTLINES OF BORDER AND HOMELAND SECURITY

Submitted By:
The National Native American Law Enforcement Association
The National Congress of American Indians

Final Report
March 31, 2006

THE NATIONAL NATIVE AMERICAN
LAW ENFORCEMENT ASSOCIATION

Washington, DC
November 6, 2006

Dear Colleagues and Friends:

The National Native American Law Enforcement Association ("NNALEA") is pleased and honored to share its Final Report for the "Indian Country Border Security and Tribal Interoperability Pilot Program" (more commonly known as the "TBS Pilot Program"). The TBS Pilot Program was an innovative program that not only comprehensively assessed tribal border security preparedness generally and in relation to the evolving National Preparedness Goal, but also provided a forum for national cross-jurisdictional and cross-disciplinary information sharing, collaboration, and analysis between federal, tribal, state, local, and private entities on the issues of border and homeland security.

The TBS Pilot Program is generally summarized in the Final Report. The Final Report also sets forth certain categories of information gathered from the forty (40) Tribes that participated in the TBS Pilot Program. More particularly, the Final Report sets forth six (6) general tribal views on border security in relation to homeland security that were derived from the information gathered from the Tribes who participated in the TBS Pilot Program. In addition, the Final Report sets forth twenty (20) baselines for comparison, thirty-eight (38) best practices and forty-seven (47) alerts on border security generally and border security in relation to the National Preparedness Goal. The border security best practices are practices of some of the participating Tribes that all entities may want to employ in their pursuit of border and homeland security; while the border security alerts identify border security issues that should receive immediate attention from the applicable government decision makers.

Much gratitude is extended to the participating Tribes, as their participation and completion of the TBS Pilot Program marked an important step in our Country's comprehensive assessment of its border and homeland security preparedness. Much gratitude is also extended to the many partners and friends of NNALEA who contributed to the TBS Pilot Program, with special thanks to the National Congress of American Indians and Fort Lewis College. Finally, much gratitude is extended to the Department of Homeland Security for its role in the TBS Pilot Program.

We sincerely hope that after reading the TBS Pilot Program Final Report, you too will better understand and appreciate the importance of Tribes at the frontlines of border and homeland security.

Sincerely yours,

Kim M. Baglio
President
NNALEA

Ronald Reagan Building, International Trade Center • 300 Pennsylvania Avenue Suite 700 • Washington, DC 20004
(202) 204-3065 • Fax (202) 204-3066 • www.nnalea.org

Many Thanks To:

The National Native American Law Enforcement Association (NNALEA) is deeply grateful to the many individuals and organizations who contributed to the success of the "Indian Country Border Security and Tribal Interoperability Pilot Program," also known as the Tribal Border Security Pilot Program or TBS Program.

Participating Tribes

First and foremost, we would like to thank the forty Native American Tribes and Nations which participated in the study and who are on the front lines of our border security. In addition to providing the data which laid the basis for the study, tribal leaders gave graciously of their time and expertise, coming together on a number of occasions to confer and provide further insight into the performance of the Program. Without the assistance and support of these Tribes and Nations this study would literally not have been possible. Therefore, NNALEA would like to extend a special thanks to the respective Tribal Chairpersons, Presidents, leaders, Tribal Councils, Tribal Managers, their professional staffs and the citizens of the forty Tribal Communities.

Aroostook Band of Micmac Indians - Micmac Reservation;
Assiniboine & Sioux Tribe - Fort Peck Reservation;
Bad River Band of Lake Superior Chippewa Indians - Bad River Reservation;
Bay Mills Executive Council - Bay Mills Reservation;
Blackfeet Tribe - Blackfeet Reservation;
Campo Band of Kumeyaay Indians - Campo Indian Reservation;
Cocopah Tribal Council - Cocopah Reservation;
Confederated Tribes of the Colville Reservation - Colville Reservation;
Grand Portage Band of Chippewa Indians - Grand Portage Reservation;
Grand Traverse Band of Ottawa & Chippewa - Grand Traverse Reservation;
Houlton Maliseet Band of Indians - Houlton Maliseet Reservation;
Jamestown S'Klallam Tribe - Jamestown S'Klallam Reservation;
Keweenaw Bay Indian Community - L'Anse Reservation;
Kickapoo Tribe of Texas - Kickapoo Reservation;
Kootenai Tribe - Kootenai Reservation;
Little Traverse Bay Bands of Odawa Indians - Little Traverse Bay Reservation;
Lower Elwha S'klallam Tribe - Lower Elwha S'Klallam Reservation;
Lummi Indian Tribe - Lummi Reservation;
Makah Indian Tribe - Makah Reservation;
Nooksack Indian Tribe - Nooksack Reservation;
Passamaquoddy Tribe – Indian Township Reservation;
Passamaquoddy Tribe - Pleasant Point Reservation;
Penobscot Indian Nation - Penobscot Reservation;
Port Gamble S'Klallam Tribe - Port Gamble Indian Community;
Quechan Tribe - Ft. Yuma Reservation;
Quinault Nation - Quinault Reservation;
Red Cliff Band of Lake Superior Chippewa - Red Cliff Reservation;
Red Lake Nation - Red Lake Reservation;
Saginaw Chippewa Indian Tribe - Isabella Reservation;
Sault St. Marie Tribe of Chippewa Indians - Sault Ste. Marie Reservation;
Seneca Nation - Cattaraugus Reservation;
Stillaquamish Indian Tribe - Stillaquamish Reservation;
St. Regis Mohawk Tribe - Saint Regis Mohawk Reservation;
Suquamish Indian Tribe - Port Madison Reservation;
Swinomish Tribe - Swinomish Tribal Community;
Tigual Pueblo Tribe - Ysleta Del Sur Reservation;
Tulalip Tribe - Tulalip Reservation;
Turtle Mountain Band of Chippewa Indians - Turtle Mountain Reservation;
Tuscarora Nation - Tuscarora Reservation; and
Upper Skagit Tribe - Upper Skagit Reservation

(many thanks, continued)

The National Native American Law Enforcement Association extends a special thanks to:

The "Best Practice" Tribes who graciously hosted site visits:
Cocopah Tribe of Arizona

Sault Ste. Marie Tribe of Chippewa Indians of Michigan

The Tribes who field-tested the Tribal Border Security Program research tool prior to the commencement of the survey:

Seminole Tribe of Florida
Southern Ute Indian Tribe

Thank You to Our Primary Partners:

*The **Department of Homeland Security** (DHS) for their vision in seeing the value of Native American Tribes and Nations in securing our country's borders and the United States of America.*

*The **National Congress of American Indians (NCAI),** who partnered with us to conduct this study. We are grateful to the organization as well as to the following individuals for engaging in this successful collaborative effort:*

Joe Garcia, President, NCAI and Governor, Ohkay Owingeh

Tex Hall, Former President, NCAI and Chairman,
Three Affiliated Tribes of Mandan, Hidatsa & Arikara Nation

Jacqueline Johnson, Executive Director, NCAI

Robert Holden, Director of Emergency Management and Radioactive Waste Programs, NCAI

Heather Dawn Thompson, Director of Government Affairs, NCAI

*And the **Native American Consulting Group (NACG)**, who partnered with us in the overall management of the Tribal Border Security Pilot Project. We are grateful to the organization and its expert, professional staff.*

Other Key Partners

*We also extend our appreciation to the **U.S. Department of the Interior, U.S. Department of Health & Human Services, U.S. Department of Justice, U.S. Environmental Protection Agency, and the U.S. Department of State** for their direct and indirect support throughout the Tribal Border Security Pilot Program.*

NNALEA acknowledges the many other federal, state, local and private industry departments, agencies, organizations and Tribal communities which provided invaluable assistance, including the following Tribal Border Security Advisory Committees: the Federal Advisory Panel; the Tribal Advisory Committee; and the State and Local Advisory Group

*We note the significant contributions of the **Bureau of Alcohol, Tobacco, Firearms & Explosives, the Bureau of Indian Affairs – Office of Justice Services, the Federal Bureau of Investigation, Indian Health Service, the United States Secret Service, the DHS Preparedness Directorate - Office of State and Local Government Coordination and the DHS Office of Grants and Training.***

*A special notable thanks to the **United States Border Patrol** without whose help and cooperation this study would not have been possible.*

(many thanks, continued)

Other Major Contributors:

We gratefully acknowledge the contributions of the following groups and their respective staffs

Fort Lewis College

Dean Richard Sax, Ph. D.

Professor Jeff Fox, Ph. D.

Professor Rick Wheelock, Ph. D.

Professor Richard Ellis, Ph. D.

East Central University of Oklahoma

Professor Steve Turner, Ph. D.

Candessa Morgan, Project Coordinator, Tribal Police Training Program

The National Native American Law Enforcement Association Tribal Border Security Pilot Project Team

We acknowledge our talented and dedicated project team:

The National Native American Law Enforcement Association Executive Board

Kim Baglio - President

Joseph Wicks - Vice President

Peter Maybee, - Sergeant At Arms

Gary Edwards - Chief Executive Officer

Jim Wooten - Chief Financial Officer

Daryll Davis - Senior Director

Dave Nicholas - Senior Director

Dewey Webb - Immediate Past President

The Tribal Border Security Pilot Program Leadership and Writing Team:

Gary Edwards, II, Esq.
Baker, Donelson, Bearman, Caldwell & Berkowitz, PC

Jeffrey Fox, Ph. D.
Faculty Consultant, Center for Instructional Design, Brigham Young University

Robert Holden
Director of Emergency Management and Radioactive Waste Programs, National Congress of American Indians

(many thanks, Project Leadership Team, continued)

Gary L. Edwards
Chief Executive Officer, National Native
American Law Enforcement Association

Martin Topper, Ph. D.
Volunteer, National Native American Law Enforcement Association

The National Native American Law Enforcement Association recognizes the law firm of **Baker, Donelson, Bearman, Caldwell & Berkowitz, P.C.**, for its counsel and assistance with the TBS Pilot Program and Final Report.

The TBS Pilot Program Staff

We are particularly grateful to the dedicated Tribal Border Security Pilot Program staff who worked tirelessly over the past two years to make this vision a reality. This project would not have come to fruition without their hard work, skill and expertise. Most notably, we highlight ***Marilyn Spoon,*** *Director of the TBSP Field Operations for her exceptional work and dedication.*

Marilyn Spoon – Director of Field Operations
Jeannette Williams – Compliance Officer
Laura Fakes
Gaylene Martinez
Luzene Hill
Sherry Kast
Peggy Topper

The Tribal Border Security Pilot Project Survey Team

Marilyn Spoon
Victoria Morris
Sandra Rolette
Shirley Ward
Debra Daugomah-Harjo
Corrine Tiger-Tsoodle
Luzene Hill
Peggy Topper

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The National Native American Law Enforcement Association ("NNALEA") and the National Congress of American Indians ("NCAI"), in conjunction with their partners and with the support of the Department of Homeland Security ("DHS") embarked upon a history-making venture called the "Indian Country Border Security and Tribal Interoperability Pilot Program" (more commonly known as the "TBS Pilot Program"). The TBS Pilot Program is an innovative program that not only comprehensively assessed tribal border security preparedness generally and in relation to the evolving National Preparedness Goal, but also provided a forum for national cross-jurisdictional and cross-disciplinary information sharing, collaboration, and analysis between federal, tribal, state, local, and private entities on the issues of border and homeland security. Accordingly, many thanks are expressed to all of the participants in the TBS Pilot Program, who so willingly answered the TBS Pilot Program's call to action -- "to stand shoulder to shoulder" in securing our great country's borders.[1]

The remainder of this Final Report is divided into sections that provide information on the following topics: (I) Tribal Border Security Background; (II) Summary of the Methodology for the TBS Pilot Program; (III) Tribal Border Security General Views, Best Practices, and Alerts Identified from the TBS Pilot Program General Survey Data; (IV) Tribal Border Security Baselines, Best Practices, and Alerts Identified from the TBS Pilot Program Specific Survey Data; (V) Tribal Border Security Best Practices and Alerts Identified during the TBS Pilot Program Site Visits; and (VI) Concluding Remarks. Notably, in the aggregate, this Final Report sets forth six (6) general tribal views on border security in relation to homeland security, as well as twenty (20) baselines for comparison, thirty-eight (38) best practices,[2] and forty-seven (47) alerts[3] on border security generally and border security in relation to the National Preparedness Goal. By participating in the TBS Pilot Program, the participating border Tribes have taken another major step toward securing their respective communities as well as securing America as a whole.

Subsequent programs lawfully patterned after the TBS Pilot Program would render a complete set of baselines, best practices, and alerts that could be used to effectively, fairly, and consistently assess preparedness and future border and homeland security investment justification initiatives. Without the performance of these additional programs, the national and uniformed preparedness standard sought, will remain elusive, thereby hampering decision makers' ability to determine the most beneficial future investment justification initiatives. It is doubtful that border and homeland security can ever be achieved at its most optimal level without this national and uniformed standard. [4]

[1] "To stand shoulder to shoulder" is a phrase coined by Senator Ben "Nighthorse" Campbell.
[2] The border security best practices are practices that all entities may want to employ in their pursuit of border and homeland security.
[3] The border security alerts identify border security issues that should receive immediate attention from the applicable government decision makers.
[4] The statements set forth in this Final Report are those of the authors of this Final Report, and are not necessarily the statements of others such as the Department of Homeland Security.

FINAL REPORT

I. TRIBAL BORDER SECURITY BACKGROUND.

Enhancing the security of the U.S. borders with Mexico and Canada has emerged as a significant policy issue.[1] President George W. Bush recently stated that "[s]ecuring our border is essential to securing the homeland."[2] President Bush further stated that "our responsibility is clear: We are going to protect the border."[3]

Since the mid-1990s "attention and resources directed at deterring and preventing illegal aliens, drug smugglers, potential terrorists, and other criminals seeking to enter the United States illegally across its land borders have risen."[4] This rise was fueled by the September 11, 2001 terrorist attacks in conjunction with reports such as the following:

> "In December 1999, Ahmed Ressam, a terrorist trained in Osama bin Laden's Afghanistan camps, was arrested shortly after crossing the border between Canada and Washington state. In the trunk of his car were explosives and other bomb-making materials. Ressam later confessed his plans to attack a variety of targets in the United States, including the Seattle Space Needle and Los Angeles Airport, as part of a wider plan to attack America during the millennium celebrations."[5]
>
> * * * * *
>
> "Recent information from ongoing investigations, detentions, and emerging threat streams strongly suggests that al-Qaeda has considered using the Southwest Border to infiltrate the United States. Several al-Qaeda leaders believe operatives can pave their way into the country through Mexico and also believe illegal entry is more advantageous than legal entry for operational security reasons."[6]

More recently, Homeland Security Secretary Michael Chertoff stated that "[r]ight now we're facing a huge challenge at the border with illegal migration."[7] This remark came on the heels of the following remarks by President Bush regarding illegal migration at the U.S. borders:

---

[1] *See Border Security Agencies Need to Better Coordinate Their Strategies and Operations on Federal Lands*, United States General Accounting Office, GAO-04-590, June 2004.
[2] *See President Discusses Border Security and Immigration Reform in Arizona*, Tucson, Arizona, Davis-Monthan Air Force Base, November 28, 2005.
[3] *Id.*
[4] *See Border Security Agencies Need to Better Coordinate Their Strategies and Operations on Federal Lands*, United States General Accounting Office, GAO-04-590, June 2004.
[5] *See In Focus: Northern Border Security*, United States Senator Debbie Stabenow (Michigan).
[6] *See Border Security Commentary*, CNSNews.com, Paul M. Weyrich, May 13, 2005, *quoting* Former Deputy Secretary of Homeland Security Admiral James M. Loy.
[7] *See Remarks by Homeland Security Secretary Michael Chertoff on Homeland Security Accomplishments and Priorities*, U.S. Department of Homeland Security, December 20, 2005.

> Illegal immigration puts pressure on our schools and hospitals.[1]
>
> * * * * *
>
> . . . it [illegal immigration] strains the resources needed for law enforcement and emergency services.[2]
>
> * * * * *
>
> . . . smugglers and gangs that bring illegal immigrants across the border also bring crime to our neighborhoods and danger to the highways.[3]

Statistics from 2005 support the comments of both President Bush and Homeland Security Secretary Chertoff. More particularly, in 2005, over one million illegal immigrants were caught attempting to enter the United States at its borders, and over $100 million in counterfeit goods and over two million pounds of illegal drugs were seized at the U.S. borders.[4] One is only left to ponder about "who" and "what" were not caught and seized respectively.

Not surprisingly, the Department of Homeland Security has concluded that the smuggling of illegal immigrants into the United States constitutes a significant risk to national security and public safety.[5] In addition, smuggling pipelines which are used by illegal immigrants and criminals seeking to enter the United States may also be used by terrorists.[6] It is estimated that the illegal immigrant smuggling and sex trafficking trade generates $9.5 billion for criminal organizations worldwide, and the profits are used to finance additional criminal enterprises such as: the trafficking of drugs, weapons, and other contraband; the commission of collateral crimes such as kidnapping, homicide, assault, rape, robbery, auto theft, high speed flight, identity theft, and the manufacturing and distribution of fraudulent documents; and the perpetuation of terrorist acts.[7] Further, "[t]he illicit drug trade is a billion-dollar business that often involves the perpetration of violent crimes," and "Mexico is a major corridor for the transport of illicit drugs to the United States."[8]

The attention and resources available to prevent, protect, respond, and recover from such illegal migration, drug smuggling, potential terrorism, and crime is spread

---

[1] *See President Discusses Border Security and Immigration Reform in Arizona*, Tucson, Arizona, Davis-Monthan Air Force Base, November 28, 2005.
[2] *Id.*
[3] *Id.*
[4] *See Remarks by Homeland Security Secretary Michael Chertoff on Homeland Security Accomplishments and Priorities*, U.S. Department of Homeland Security, December 20, 2005.
[5] *See Border Security and the Southwest Border: Background, Legislation, and Issues*, CRS Report for Congress, Order Code RL33106, September 28, 2005.
[6] *Id.*
[7] *See Border Security and the Southwest Border: Background, Legislation, and Issues*, CRS Report for Congress, Order Code RL33106, September 28, 2005.
[8] *Id.*

across approximately 5,900 miles of U.S. borders.[1] This 5,900 miles of U.S. borders is comprised of approximately 1,900 miles of border with Mexico (the "Southern Border"), and approximately 4,000 miles of border with Canada (the "Northern Border").[2] Certain characteristics regarding these U.S. borders are rather common knowledge.

For instance, with regard to the Southern Border it is common knowledge that it is comprised of six Mexican and four U.S. states.[3] The U.S. states are California, Arizona, New Mexico, and Texas.[4] This border is comprised of large tracts of desert land with sweltering heat, mountain ranges and other rugged terrain, and rivers (i.e., Colorado River and the Rio Grande River).[5] In addition, the Southern Border has a longstanding history of illegal migration and human and drug smuggling activities, and therefore, the historic focus of border security on this border has primarily been on stemming illegal migration, human smuggling, and interdicting illegal drugs.[6]

Likewise, with regard to the Northern Border it is common knowledge that it is comprised of seven Canadian provinces and ten U.S. states.[7] The U.S. states are Washington, Idaho, Montana, North Dakota, Minnesota, Michigan, New York, Vermont, New Hampshire, and Maine.[8] This border is comprised of vast mountain ranges (i.e., the Rockies), the Great Lakes, many different river systems, and heavy snow and bitter cold temperatures in the winter.[9] Historically, the Northern Border has experienced illegal migration and human and drug smuggling activities on a smaller scale than that experienced on the Southern Border. In addition, the United States and Canada have emphasized sharing information, streamlining policies, and facilitating trade.[10]

What, however, may not be common knowledge with regard to the Southern Border and the Northern Border, is that "[o]f the 562 federally recognized Indian tribes, 36 tribes have lands that are close to, adjacent to, or crosses over international boundaries with Mexico or Canada."[11] These 36 tribes, therefore, are on the frontlines of protecting U.S. borders, thereby making them an integral part of border security.

Perhaps even more important, though, is the fact that the success of national border security may ultimately hinge on the ability to protect the U.S. borders to which these tribes' lands are adjacent or in close proximity. The reason for this is that as tribal

---

[1] *See Border Security Agencies Need to Better Coordinate Their Strategies and Operations on Federal Lands*, United States General Accounting Office, GAO-04-590, June 2004.
[2] *Id.*
[3] *Border Security and the Southwest Border: Background, Legislation, and Issues*, CRS Report for Congress, Order Code RL33106, September 28, 2005.
[4] *Id.*
[5] *Id.*
[6] *Id.*
[7] *Id.*
[8] *Id.*
[9] *Id.*
[10] *Id.*
[11] *See Border Security Agencies Need to Better Coordinate Their Strategies and Operations on Federal Lands*, United States General Accounting Office, GAO-04-590, June 2004.

communities rank at or near the bottom of nearly every social, health and economic indicator,[1] and as tribal communities are confronted with rather complex, misunderstood and confusing jurisdiction issues,[2] their tribal lands and the borders to which their lands are adjacent or in close proximity may only be minimally protected. As a result, a significant number of the undetected border security breaches achieved by illegal aliens, drug smugglers, potential terrorists, and criminals may be occurring across these borders and tribal lands. In addition, as border patrol efforts and resources are increased in the more populated areas (i.e., in non-tribal lands), more illegal traffic may very well be routed through these more remote tribal lands and borders.[3]

In recognition of the importance that tribes play in protecting the U.S. borders, the United States Department of Homeland Security ("DHS"), in consultation with the National Native American Law Enforcement Association ("NNALEA") and the National Congress of American Indians ("NCAI") devised the "Indian Country Border Security and Tribal Interoperability Pilot Program," more commonly referred to as the TBS Pilot Program. One of the primary goals of the TBS Pilot Program was to comprehensively assess the preparedness of the Tribes who have lands adjacent to or in close proximity to the Southern Border and the Northern Border of the United States.

As the TBS Pilot Program was evolving, so too was the National Preparedness Goal (the "Goal"), the interim version of which was introduced by the Department of Homeland Security ("DHS") in 2005. The Goal established a framework that guides entities at all levels of government in the development and maintenance of the following: (1) Capabilities to prevent, protect against, respond to, and recover from major events; and (2) Capabilities to identify, prioritize, and protect critical infrastructure and key resources.[4] The Goal is to be achieved by the process of Capabilities-Based Planning.[5] This process is defined as "planning, under uncertainty, to provide capabilities suitable for a wide range of threats and hazards while working within an economic framework that necessitates prioritization and choice."[6] The Capabilities-Based Planning process provides the means for the Nation to achieve the Goal by answering three fundamental questions: "How prepared do we need to be?", "How prepared are we?", and "How do we prioritize efforts to close the gap?".[7] At the heart of the Goal and the Capabilities-Based Planning process is the Target Capabilities List (TCL).[8] The TCL identifies thirty-six (36) capabilities integral to Nation-wide all-hazards preparedness.[9]

---

[1] *See generally Existing Conditions on Indian Reservations*, Walking Shield - American Indian Society, *citing* U.S. Commission on Civil Rights July 2003 report titled *Federal Funding and Unmet Needs in Indian Country.*

[2] *See e.g.*, Public Law 280.

[3] *See generally, Border Security Agencies Need to Better Coordinate Their Strategies and Operations on Federal Lands*, United States General Accounting Office, GAO-04-590, June 2004; *see also Border Security and the Southwest Border: Background, Legislation, and Issues*, CRS Report for Congress, Order Code RL33106, September 28, 2005.

[4] *See Homeland Security Presidential Directive 8: National Preparedness*; *See also Fact Sheet -- Strengthening National Preparedness: Capabilities-Based Planning*; *Fact Sheet -- A Nation Prepared: The Target Capabilities List*; *Fact Sheet: A Common Approach to Preparedness: The National Preparedness Goal.*

[5] *Id.*

[6] *Id.*

[7] *Id.*

[8] *Id.*

[9] *Id.*

Accordingly, in assessing the preparedness of the tribes who had lands adjacent to or in close proximity to the Southern Border and the Northern Border of the United States, the TBS Pilot Program incorporated a capabilities-based planning process for its assessment that included cross-jurisdictional and cross-disciplinary elements. More specifically, the TBS Pilot Program sought to provide a means for the tribes who had lands adjacent to or in close proximity to the Southern Border and the Northern Border of the United States to provide information responsive to one of the three fundamental questions of the Goal, namely: "How prepared are we?". The idea being that not only would the information gathered from the TBS Pilot Program provide answers to this fundamental question, but also the information could subsequently be used by the respective Tribes and the Federal government to provide answers to the remaining two fundamental questions of the Goal.[1] That is, the information gathered could subsequently be used to develop plans for prioritization of resources and formal investment justification initiatives pertaining to various capabilities, particularly with regard to each Tribe's respective border and homeland security, as well as the border and homeland security of America as a whole.

Commendably, forty (40) of the forty-one (41) Tribes identified by NNALEA and NCAI as having lands adjacent to or in close proximity to the Southern Border and the Northern Border of the United States agreed to participate in the TBS Pilot Program. The affirmative answer by these forty (40) Tribes to the TBS Pilot Program's call to action re-affirmed the veracity of Senator Ben Nighthorse Campbell's statement that:

> Native People are Americans first - and want to stand shoulder to shoulder with the rest of their countrymen in defending American lives and homelands from the threats now before us.

As President Bush recently stated: "America is grateful to those who are on the front lines of enforcing the border."[2] This statement applies equally to these Tribes.

[1] The "remaining two fundamental questions of the Goal" referenced in this sentence are: "How prepared do we need to be?" and "How do we prioritize efforts to close the gap?".

[2] *See President Discusses Border Security and Immigration Reform in Arizona*, Tucson, Arizona, Davis-Monthan Air Force Base, November 28, 2005.

II. SUMMARY OF THE METHODOLOGY FOR THE TBS PILOT PROGRAM.

The ultimate design for the TBS Pilot Program entailed the following two (2) primary elements: (a) Selection and Rallying of the Tribes for the Program; and (b) Information Sharing and Capabilities Analysis in the Program. Each is discussed in turn.

A. Selection and Rallying of the Tribes for the TBS Pilot Program.

The first primary element of the design of the TBS Pilot Program concerned the selection and rallying of the Tribes for the Program. The criteria used for selecting the Tribes to participate in the TBS Pilot Program were two-fold: (a) Each Tribe had to be a federally recognized Tribe; and (b) Each Tribe had to have tribal lands located within 100 miles of either the U.S. border with Canada or the U.S. border with Mexico. Using these criteria, the TBS Pilot Program partners researched the possible universe of Tribes for the Program, and concluded that there were forty-one (41) Tribes who met the criteria. Accordingly, the TBS Pilot Program partners extended invitations to all forty-one (41) of the identified Tribes to participate in the TBS Pilot Program. Commendably, of these forty-one (41) Tribes, forty (40) Tribes graciously agreed to participate in the Program, namely:

1. Aroostook Band of Micmac Indians - Micmac Reservation;
2 Assiniboine & Sioux Tribe - Fort Peck Reservation;
3. Bad River Band of Lake Superior Chippewa Indians - Bad River Reservation;
4. Bay Mills Executive Council - Bay Mills Reservation;
5. Blackfeet Tribe - Blackfeet Reservation;
6. Campo Band of Kumeyaay Indians - Campo Indian Reservation;
7. Cocopah Tribal Council - Cocopah Reservation;
8. Confederated Tribes of the Colville Reservation - Colville Reservation;
9. Grand Portage Band of Chippewa Indians - Grand Portage Reservation;
10. Grand Traverse Band of Ottawa & Chippewa - Grand Traverse Reservation;
11. Houlton Maliseet Band of Indians - Houlton Maliseet Reservation;
12. Jamestown S'Klallam Tribe - Jamestown S'Klallam Reservation;
13. Keweenaw Bay Indian Community - L'Anse Reservation;
14. Kickapoo Tribe of Texas - Kickapoo Reservation;
15. Kootenai Tribe - Kootenai Reservation;
16. Little Traverse Bay Bands of Odawa Indians - Little Traverse Bay Reservation;
17. Lower Elwha S'klallam Tribe - Lower Elwha S'Klallam Reservation;
18. Lummi Indian Tribe - Lummi Reservation;
19. Makah Indian Tribe - Makah Reservation;
20. Nooksack Indian Tribe - Nooksack Reservation;
21. Passamaquoddy Tribe – Indian Township Reservation;
22. Passamaquoddy Tribe - Pleasant Point Reservation;
23. Penobscot Indian Nation - Penobscot Reservation;
24. Port Gamble S'Klallam Tribe - Port Gamble Indian Community;
25. Quechan Tribe - Ft. Yuma Reservation;
26. Quinault Nation - Quinault Reservation;
27. Red Cliff Band of Lake Superior Chippewa - Red Cliff Reservation;
28. Red Lake Nation - Red Lake Reservation;
29. Saginaw Chippewa Indian Tribe - Isabella Reservation;
30. Sault St. Marie Tribe of Chippewa Indians - Sault Ste. Marie Reservation;
31. Seneca Nation - Cattaraugus Reservation;

32. Stillaquamish Indian Tribe - Stillaquamish Reservation;
33. St. Regis Mohawk Tribe - Saint Regis Mohawk Reservation;
34. Suquamish Indian Tribe - Port Madison Reservation;
35. Swinomish Tribe - Swinomish Tribal Community;
36. Tigual Pueblo Tribe - Ysleta Del Sur Reservation;
37. Tulalip Tribe - Tulalip Reservation;
38. Turtle Mountain Band of Chippewa Indians - Turtle Mountain Reservation;
39. Tuscarora Nation - Tuscarora Reservation; and
40. Upper Skagit Tribe - Upper Skagit Reservation.

On multiple occasions during the course of the TBS Pilot Program, tribal leaders from the majority of these participating Tribes were brought together to confer on the status of the TBS Pilot Program, to provide insight into the performance of the Program, and to demonstrate support for the Program.

B. Information Sharing and Capabilities Analysis in the TBS Pilot Program.

The second primary element of the design of the TBS Pilot Program concerned the information sharing and capabilities analysis in the Program. This element was achieved through a General Survey, a Specific Survey, and Site Visits -- all of which are discussed in more detail below.

1. TBS Pilot Program General Survey.

The General Survey was the data collection instrument devised for the TBS Pilot Program to collect information from the forty (40) participating border Tribes on the issue of border security in relation to homeland security. The General Survey employed a subjective format consisting of seven (7) questions to which narrative answers were requested from each participating Tribe. Administration of the General Survey was accomplished by first contacting the appropriate tribal leaders and members of each participating Tribe about the General Survey, and thereafter mailing a copy of the General Survey to each participating Tribe for completion. Commendably, all forty (40) of the participating Tribes completed the General Survey. The information shared by the participating border Tribes in response to the questions of the General Survey were compiled into a usable computer data set. The data was then analyzed in the aggregate for general views, best practices, and alerts concerning tribal border security in relation to homeland security.[1] It is anticipated that this data can also be used to compare the subjective views, best practices, and alerts contained therein, with the objective baselines, best practices, and alerts identified from the data generated from the Specific Survey.[2]

2. TBS Pilot Program Specific Survey.

The Specific Survey was the data collection instrument devised for the TBS Pilot Program to collect information from the forty (40) participating border Tribes on the issues of border security generally and border security in relation to the National Preparedness Goal. The Specific Survey employed an objective format consisting of the following six

[1] That data analysis from the General Survey is discussed in Section III, *infra*.
[2] The Specific Survey is discussed below.

(6) Sections: (a) Emergency Management and Public Works; (b) Law Enforcement, Border Security, and Detention Facilities; (c) Emergency Fire Responders; (d) Emergency Medical Responders and Facilities; (e) Critical Infrastructure and Environment; and (f) Public Safety Communications and Interoperability. Each Section contained numerous questions relevant to the topic of each respective Section.

Several Task Forces were formed to assist in the development and formulation of the questions to be included in each Section of the Specific Survey. The Task Forces included a federal agency advisory panel, a tribal advisory committee, and a state and local advisory committee. The federal agency advisory panel was comprised of members from a number of federal departments, entities, agencies, and associations. The tribal advisory committee was comprised of a number of tribal leaders, members of NCAI, and members of NNALEA. The state and local advisory committee was comprised of members from a number of state and/or local departments, entities, agencies, and associations. Each task force met on a number of occasions to brainstorm regarding areas to be covered by the Specific Survey, to engage in round-table discussions regarding the Specific Survey, and to assist in formulating the questions to be included in the Specific Survey.

In addition to the Task Forces, Fort Lewis College was engaged to provide technical and analytical assistance with regard to the Specific Survey. More particularly, Fort Lewis College's participation in the TBS Pilot Program included the following: (a) formulation of a peer review committee to review drafts of the Specific Survey and to provide technical and scientific recommendations for the Specific Survey; (b) selection of an established scientific database for systematically arranging the information obtained via the Specific Survey into usable data; (c) quantification of the data compiled from the information shared by the participating Tribes in response to the Specific Survey; (d) assistance in arranging information from the Specific Survey into usable data by performing compilations and analyses for each participating Tribe and for all participating Tribes in the aggregate; and (e) assistance with this Final Report for the TBS Pilot Program.

Once an initial draft of the Specific Survey was prepared, the first of two (2) peer tests was performed. The Southern Ute Tribe graciously agreed to participate in and to host the first peer test. Accordingly, the Southern Ute Tribe shared their information in response to the questions of the Specific Survey. In addition, the Southern Ute Tribe provided feedback on the Specific Survey, as well as recommendations for subsequent versions of the Specific Survey.

After the first peer test of the Specific Survey was completed, the Specific Survey, along with the answers and recommendations of the Southern Ute Tribe, were sent to the Fort Lewis College Peer Review Committee for its review and recommendations. The Specific Survey was also reviewed by DHS, NNALEA, and NCAI. Thereafter, the Specific Survey was overhauled.

The second of the two (2) peer tests was then performed on the Specific Survey. The Seminole Tribe graciously agreed to participate in and to host the second peer test. Accordingly, the Seminole Tribe shared their information in response to the questions of the Specific Survey. In addition, the Seminole Tribe provided feedback on the Specific Survey, as well as recommendations for subsequent versions of the Specific Survey.

After the second peer test of the Specific Survey was completed, the Specific Survey, along with the answers and recommendations of the Seminole Tribe, were sent to the Fort Lewis College Peer Review Committee for its review and recommendations. The Specific Survey was also reviewed by DHS, NNALEA, and NCAI. Thereafter, the Specific Survey was finalized, and copies of said Survey were made and bound.[1]

In order to safeguard the confidentiality and security of the Specific Surveys and the information contained therein, as well as to ensure the completeness of each Specific Survey, a tracking procedure was devised. This procedure utilized a specific chain of custody, a final destination secured storage site, and a written Tracking Log to document the exchanges. This tracking procedure was utilized for each Specific Survey answered by each of the forty (40) participating border Tribes.

Moreover, guidelines were developed for administering the Specific Survey to the forty (40) participating border Tribes. These guidelines included procedures and protocols to be followed by the Team Members of the TBS Pilot Program that were tasked with gathering the information being shared by the participating Tribes in response to the Specific Survey. The purpose of the guidelines was to help ensure consistent administration of the Specific Survey. After the guidelines were developed, the Team Members tasked with administering the Specific Survey were trained on the guidelines.

Subsequently, the Specific Survey was administered to the forty (40) border Tribes who agreed to participate in the TBS Pilot Program. Administration of the Specific Survey included making contact with appropriate Tribal leaders and members of each participating Tribe, engaging in numerous conference calls with these Tribal leaders and members to gather the information requested by the Specific Survey, and the performance of checks by the TBS Pilot Program Compliance Officer to ensure that each Specific Survey was completed *in toto*. Commendably, all forty (40) of the participating Tribes shared their respective information in response to all of the questions set forth in the Specific Survey.

After the information from the Specific Survey was gathered, it was quantified and entered into a SPSS (Statistical Program for the Social Sciences) statistical program and data file for analysis by the TBS Pilot Program partners. Once all of the data was entered, the database was thoroughly cleaned and checked for errors using accepted statistical methods.[2] Variances in the data were duly recorded.[3] NNALEA and its partners then identified certain special data analysis runs that were particularly relevant to border security generally and to border security in relation to the National Preparedness Goal. These data analysis special runs were then performed by Fort Lewis College, and assessed by NNALEA and its partners for border security baselines, best practices, and alerts.[4] It is anticipated that these data analyses can be used by DHS and the participating

[1] Collectively, the six (6) Sections of the finalized Specific Survey are comprised of 359 pages of questions. For more information regarding the Specific Survey, please contact NNALEA.
[2] *See Research Methods in the Social Sciences*, Franfort-Nachmias, Chava and David Nachmias, New York: St. Martin's Press (1996); *Exploratory Data Mining and Data Cleaning*, Dasu, Tamraparni and Theodore Johnson, Hoboken, NJ: Wiley (2003).
[3] Variances include missing data and errors.
[4] The data analyses are discussed in Section IV, *infra*.

Tribes to assess each Tribe's border security preparedness, as well as the border security preparedness of the participating border Tribes in the aggregate.[1]

3. TBS Pilot Program Site Visits.

Two (2) site visits were conducted in the TBS Pilot Program. The TBS Pilot Program site visit team was composed of representatives of DHS, NNALEA, and NCAI, with outstanding participation from other federal, state, local, and private entities. The purpose of the site visits was to visually observe certain tribal border security best practices and alerts identified from the information shared in the tribal responses to the General Survey and to the Specific Survey. In addition, the site visits provided a forum for the Tribes participating in the site visits to educate others on their best practices and the border security alerts that they have identified, and in turn to receive certain training and briefings from federal, state, local, and private entities. To capture a more complete picture of tribal border security with regard to the U.S. border with Canada and the U.S. border with Mexico, it was determined that one site visit should be performed with a Tribe located on or in close proximity to the U.S. border with Canada, while the second site visit should be performed with a Tribe located on or in close proximity to the U.S. border with Mexico. The Sault Ste. Marie Tribe of Chippewa Indians (whose tribal lands border the U.S. border with Canada), and the Cocopah Tribe (whose tribal lands border the U.S. Border with Mexico) graciously agreed to participate in the site visits.[2] It is believed that the border security alerts identified and examined during these site visits apply to all of the participating border Tribes who are similarly situated (i.e., in terms of geographic location) to the Tribes who were selected and agreed to participate in the site visits.

[1] For instance, a participating border Tribe can take its data generated from the Specific Survey and compare it with the baselines, best practices, and alerts identified from the data generated from all of the participating border Tribes, and therefrom assess its level of border security preparedness in relation to its border Tribe brethren. It should be noted, however, that as the TBS Pilot Program is the first of its kind, there is apparently not any border security baselines, best practices, or alerts that have been generated on a national level and to which compatible comparisons can be made (i.e., between national border security preparedness and each participating border Tribe's preparedness; between national border security preparedness and the participating border Tribes' preparedness in the aggregate). In this regard, the forty (40) participating border Tribes have not only distinguished themselves as leaders in border security, but also have propelled themselves to the front of the line with regard to border security preparedness initiatives.

[2] The site visits are discussed in more detail in Section V, *infra*.

III. TRIBAL BORDER SECURITY GENERAL VIEWS, BEST PRACTICES, AND ALERTS IDENTIFIED FROM THE TBS PILOT PROGRAM GENERAL SURVEY DATA.

The data compiled from the information shared by the forty (40) participating border Tribes in response to the General Survey of the TBS Pilot Program reveals certain general tribal border security views, best practices, and alerts. These views, best practices, and alerts are detailed below.

A. General Tribal Border Security Views.

The information shared by the participating Tribes in response to the General Survey in the TBS Pilot Program reveals a number of general tribal border security views. It should be noted, however, that these views are subjective responses to the open-ended questions of the General Survey, and therefore, may not be as comprehensive as the data set forth in Section IV, *infra*.[1]

One tribal border security general view pertains to the participating Tribes' perception of their respective role in the national strategy for homeland security. 60% of the participating border Tribes reported that they fully understand their role in the national strategy for homeland security, with an additional 10% reporting that they partially understand their role.

A second tribal border security general view pertains to the participating Tribes' perception of their respective preparedness and capabilities to prevent threats or acts of terrorism, natural disasters and other national emergencies from occurring in their respective communities and/or through their respective borders. Only four (4) of the forty (40) participating border Tribes reported that they are sufficiently prepared and capable to so prevent. The reasons identified for the insufficient preparedness and capabilities are deficiencies in funding, personnel, training, equipment, communications, and information.

A third tribal border security general view pertains to the participating Tribes' perception of their respective preparedness and capabilities to respond to threats or acts of terrorism, natural disasters and other national emergencies. Only three (3) of the forty (40) participating border Tribes reported that they are sufficiently prepared and capable to so respond. The reasons identified for the insufficient preparedness and capabilities are deficiencies in funding, personnel, training, equipment, communications, and planning.

A fourth tribal border security general view pertains to the participating Tribes' perception of their respective preparedness and capabilities to recover from threats or acts of terrorism, natural disasters and other national emergencies that occur in their respective communities and/or through their respective borders. Only one (1) of the forty (40) participating border Tribes reported that it is sufficiently prepared and capable to so recover. The reasons identified for the insufficient preparedness and capabilities are deficiencies in funding, personnel, training, equipment, and planning.

[1] Section IV, *infra*, pertains to the data compiled from the TBS Pilot Program Specific Survey.

A fifth tribal border security general view pertains to the participating Tribes' perception of their respective general understanding regarding the National Incident Management System (NIMS).[1] 70% of the participating border Tribes reported that they have a full general understanding of NIMS, with an additional 7.5% reporting that they have a partial general understanding of NIMS.

A sixth tribal border security general view pertains to the participating Tribes' perception of their respective general understanding regarding the National Response Plan (NRP). 50% of the participating border Tribes reported that they have a full general understanding of the NRP, with an additional 7.5% reporting that they have a partial general understanding of the NRP.

B. General Tribal Border Security Best Practices.

The information shared by the participating Tribes in response to the General Survey in the TBS Pilot Program reveals a number of general tribal border security best practices. One tribal border security best practice pertains to the participating border Tribes who view their role in the National Strategy for Homeland Security as including interaction with local, state, and federal entities (i.e., as opposed to just intra-tribal interaction). A second tribal border security best practice pertains to the participating border Tribes who have existing relationships with local entities (75% of the participating border Tribes reported such), state entities (65% of the participating border Tribes reported such), and/or federal entities (45% of the participating border Tribes reported such). A third tribal border security best practice pertains to the participating border Tribes who perceive that the U.S. Customs and Border Protection are available to assist the border Tribes (10% of the participating border Tribes indicated such).

C. General Tribal Border Security Alerts.

The information shared by the participating Tribes in response to the General Survey in the TBS Pilot Program reveals several general tribal border security alerts. One tribal border security alert is that 40% of the participating border Tribes indicated that they do not fully understand their role in the national strategy for homeland security. A second border security alert is that 90% of the participating border Tribes indicated that they were not sufficiently prepared and capable to prevent threats or acts of terrorism, natural disasters and other national emergencies from occurring in their respective communities and/or through their respective borders. A third border security alert is that 92.5% of the participating border Tribes indicated that they were not sufficiently prepared and capable to respond to threats or acts of terrorism, natural disasters and other national emergencies. A fourth border security alert is that 97.5% of the participating border Tribes indicated that they were not sufficiently prepared and capable to recover from threats or acts of terrorism, natural disasters and other national emergencies that occur in their respective communities and/or through their respective borders. A fifth border security alert is that funding and training deficiencies are the two (2) most prevalent limitations cited by the participating border Tribes to their respective abilities to prevent, respond to, and recover

[1] NIMS is a system mandated by HSPD-5 that provides a consistent, nationwide approach for federal, state, local, and tribal governments; the private sector; and nongovernmental organizations to work effectively and efficiently together to prepare for, respond to, and recover from domestic incidents, regardless of cause, size, or complexity. To provide for interoperability and compatibility among federal, state, local, and tribal capabilities, the NIMS includes a core set of concepts, principles, and terminology. HSPD-5 identifies these as the ICS; multi-agency coordination systems; training; identification and management of resources (including systems for classifying types of resources); qualification and certification; and the collection, tracking, and reporting of incident information and incident resources.

from threats or acts of terrorism, natural disasters and other national emergencies. A sixth border security alert is that in addition to funding and training deficiencies, personnel and equipment deficiencies are the other primary limitations cited by the participating border Tribes to their respective abilities to prevent, respond to, and recover from threats or acts of terrorism, natural disasters and other national emergencies. A seventh border security alert is that 30% of the participating border Tribes reported that they do not have a full general understanding of NIMS. Finally, an eighth border security alert is that 50% of the participating border Tribes reported that they do not have a full general understanding of the NRP.

IV. TRIBAL BORDER SECURITY BASELINES, BEST PRACTICES, AND ALERTS IDENTIFIED FROM THE TBS PILOT PROGRAM SPECIFIC SURVEY DATA.

A voluminous amount of data was compiled from the information shared by the forty (40) participating border Tribes in response to the Specific Survey of the TBS Pilot Program. From this data, multiple baselines can be established, and multiple best practices and alerts can be analyzed. The scope of the TBS Pilot Program, however, was limited to border homeland security, and therefore, the baselines, best practices, and alerts set forth herein pertain primarily to border homeland security. More particularly, the border security baselines, best practices, and alerts set forth herein were generated from the compiled data that was deemed to be most relevant to border security in the following two (2) contexts: (1) border security generally; and (2) border security in relation to the National Preparedness Goal. In the context of border security generally, the baselines, best practices, and alerts pertain to non-native border crossings, smuggling activities that have been encountered by the border Tribes, the entities providing border patrols, and the existence of specific strategies for border protection. In the context of border security in relation to the National Preparedness Goal, the baselines, best practices, and alerts pertain to two (2) functions (namely, preparedness, and communications and information management) of the Department of Homeland Security's common target tasks and capabilities, as well as to critical infrastructure identification, prioritization, and protection.[1] The border security baselines, best practices, and alerts for the participating border Tribes is detailed below.

Border Security Generally

In the TBS Pilot Program, the forty (40) participating Tribes shared information pertaining to border security generally. The information shared, when analyzed in the aggregate, reveals certain tribal border security baselines, best practices and alerts.

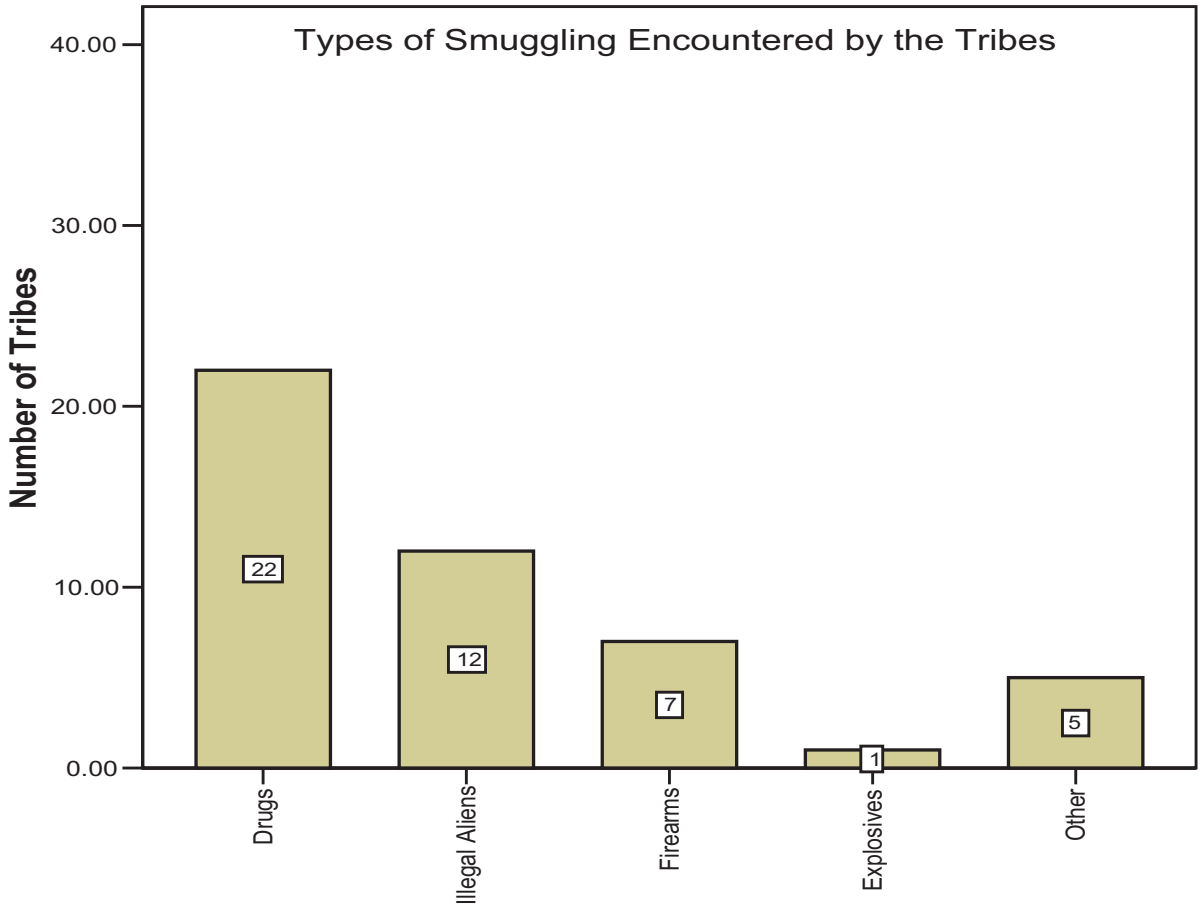
A. Tribal Border Security General Baselines.

The information shared by the participating Tribes in the TBS Pilot Program reveals a number of general tribal border security baselines. Two (2) such baselines include: (a) A baseline for comparison concerning the types of smuggling activities being encountered by the border Tribes; and (b) A baseline for comparison concerning the entities patrolling the borders of the participating Tribes.

With regard to the baseline for comparison concerning the types of smuggling activities being encountered by the border Tribes, the forty (40) participating Tribes were surveyed concerning the types of smuggling activities that they each have encountered. The specific types of smuggling activities included in the survey were the following: drugs, illegal aliens, firearms, explosives, weapons of mass destruction, and biological agents, among others. Graph 1, page 16, depicts the number of Tribes who reported encountering each type of smuggling activity.

[1] See Target Capabilities List: Version 1.1, U.S. Department of Homeland Security, May 23, 2005, pp. 12 and 49.

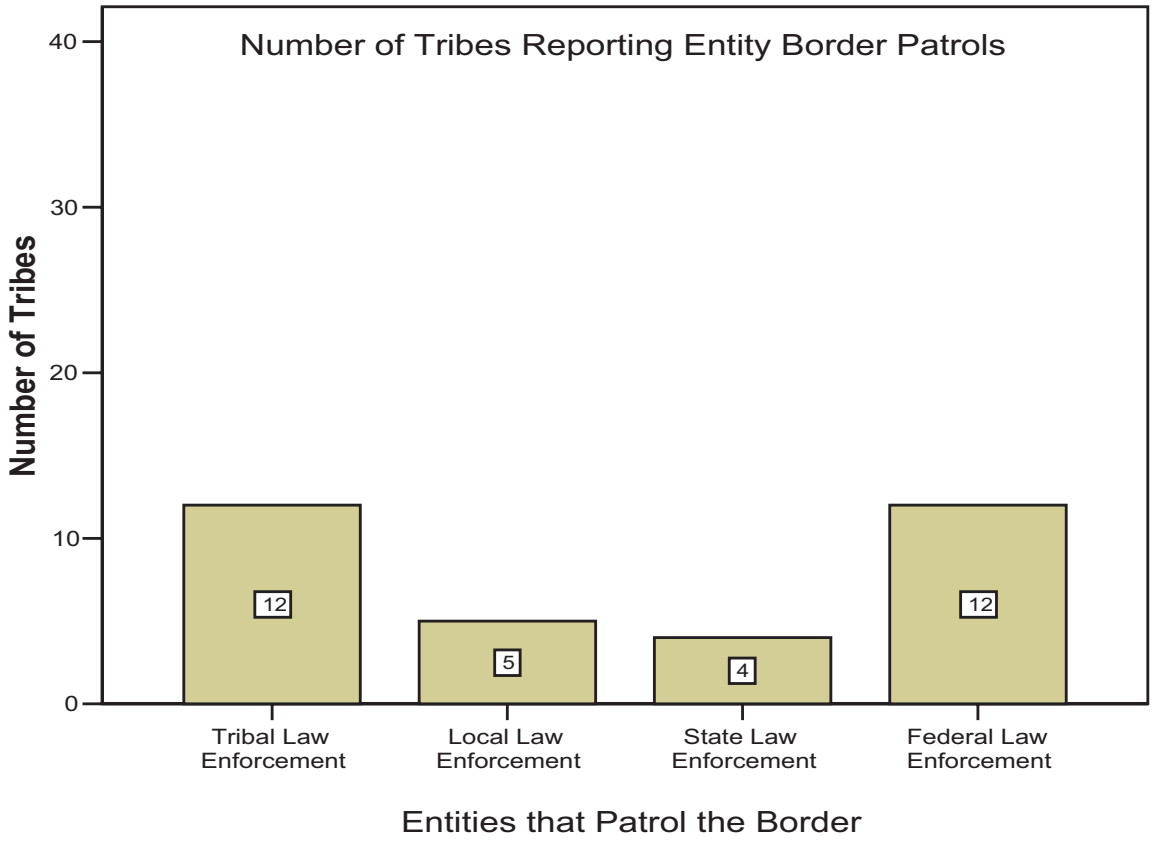
Graph 1



As depicted in Graph 1, the most common type of smuggling activity that has been encountered by the border Tribes is the smuggling of drugs.

With regard to the baseline for comparison concerning the entities patrolling the borders of the participating Tribes, the forty (40) participating tribes were surveyed concerning the types of entities who were patrolling their respective borders. The specific entities inquired about included: the tribe's law enforcement, local law enforcement, state law enforcement, and federal law enforcement. Graph 2, page 17, depicts the number of tribes who reported border patrols by each of the entities.

Graph 2



As revealed in Graph 2, the entities providing the majority of the border patrols are the tribal and federal law enforcement entities.

B. Tribal Border Security General Best Practices.

The information shared by the participating Tribes in the TBS Pilot Program reveals a couple of general tribal border security best practices. One best practice pertains to those border Tribes who have developed and implemented a specific strategy for protecting their respective borders. A second best practice pertains to those border Tribes whose law enforcement routinely patrols their respective borders.

C. Tribal Border Security General Alerts.

The information shared by the participating Tribes in the TBS Pilot Program reveals a number of general tribal border security alerts. One border security alert is that the forty (40) participating Tribes reported that over 2.3 million non-natives cross their borders per year. A second border security alert is that 67.74% of the border Tribes reported that they do not have a specific strategy for protecting their respective borders. A third border security alert is that many border Tribes reported that no patrols of their respective borders were being performed on a regular basis. Finally, a fourth border security alert is that at least one border Tribe has already encountered the smuggling of weapons of mass destruction, biological agents, and explosives.

Border Security In Terms Of The National Preparedness Goal: Preparedness

Preparedness is a function that falls within the Department of Homeland Security's common target tasks and capabilities, and therefore, is relevant in assessing border security in terms of the evolving Target Capabilities List.[1] Preparedness is the ability to "[b]uild, sustain and improve the operational capability to prevent, protect against, respond to, and recover from domestic incidents.[2] Preparedness includes organization and leadership, planning, training, exercises, resources (i.e., personnel, equipment, specialized skills/units, and facilities), and mutual aid agreements and assistance compacts.[3] The desired goal is that through preparedness a community achieves its optimal operational capability to prevent, protect against, respond to, and recover from incidents.

In the TBS Pilot Program, the forty (40) participating Tribes shared information pertaining to their respective preparedness to prevent, protect against, respond to, and recover from domestic incidents. The information shared, when analyzed in the aggregate, reveals certain tribal border security baselines, best practices, and alerts relevant to the Preparedness function. These baselines, best practices, and alerts are each summarized in turn.

A. Tribal Border Security Preparedness Baselines.

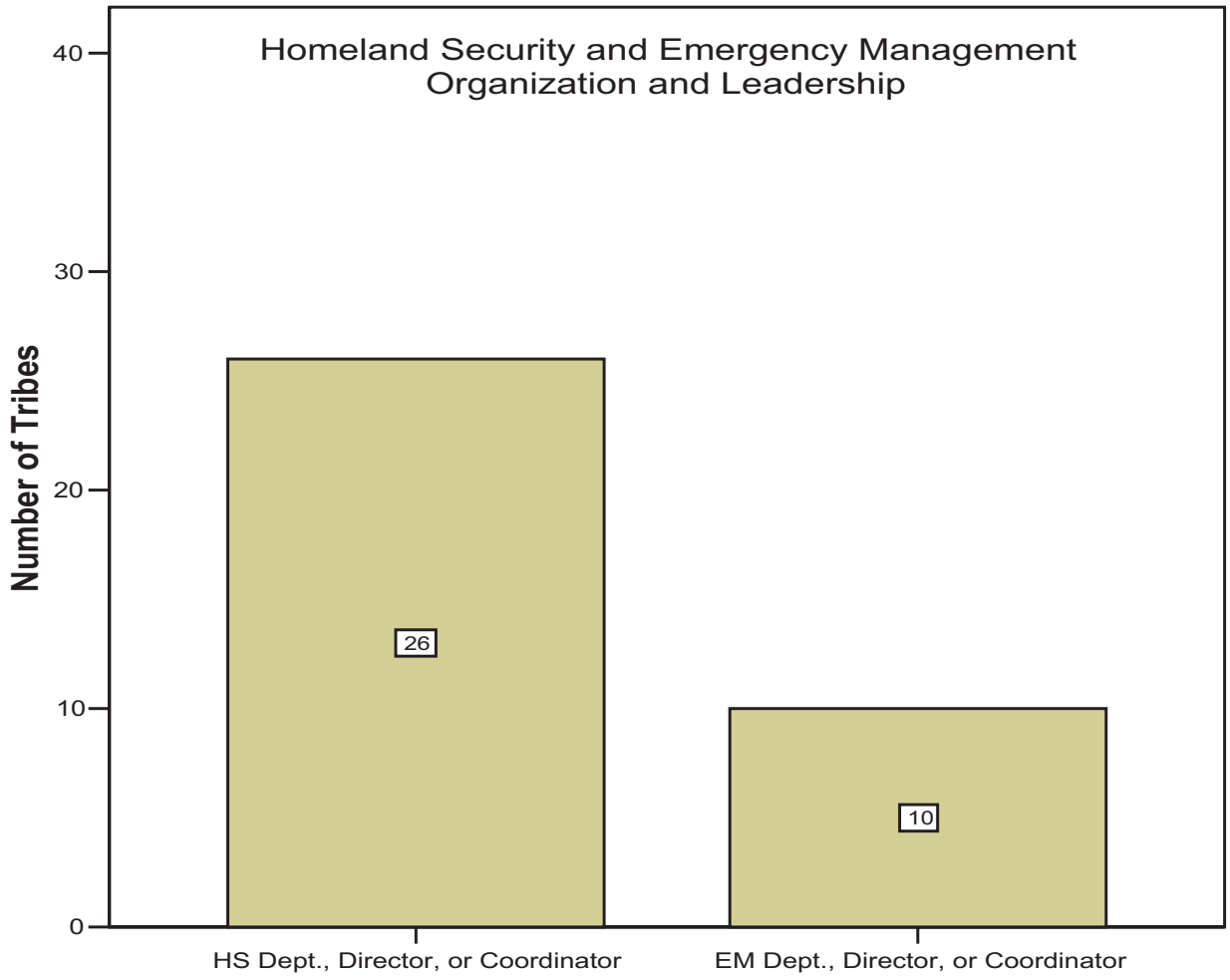
The information shared by the participating Tribes in the TBS Pilot Program reveals a number of tribal border security baselines with regard to the Preparedness function. Those baselines pertain to preparedness with regard to organization and leadership, planning, resources, training, exercises, and mutual aid and assistance compacts. These baselines are set forth below.

1. Organization and Leadership.

The organization and leadership preparedness border security baseline which the information shared by the participating border Tribes reveals is a baseline for comparison concerning the homeland security or emergency management departments, directors, and coordinators designated by the border Tribes. More particularly, the border Tribes were surveyed on whether they have a designated homeland security and/or emergency management department, director, or coordinator. Graph 3, page 19, depicts the number of Tribes reporting to possess this organization and leadership preparedness.

[1] *See Target Capabilities List: Version 1.1*, U.S. Department of Homeland Security, May 23, 2005, p. 12.
[2] *Id.*
[3] *Id.*

Graph 3



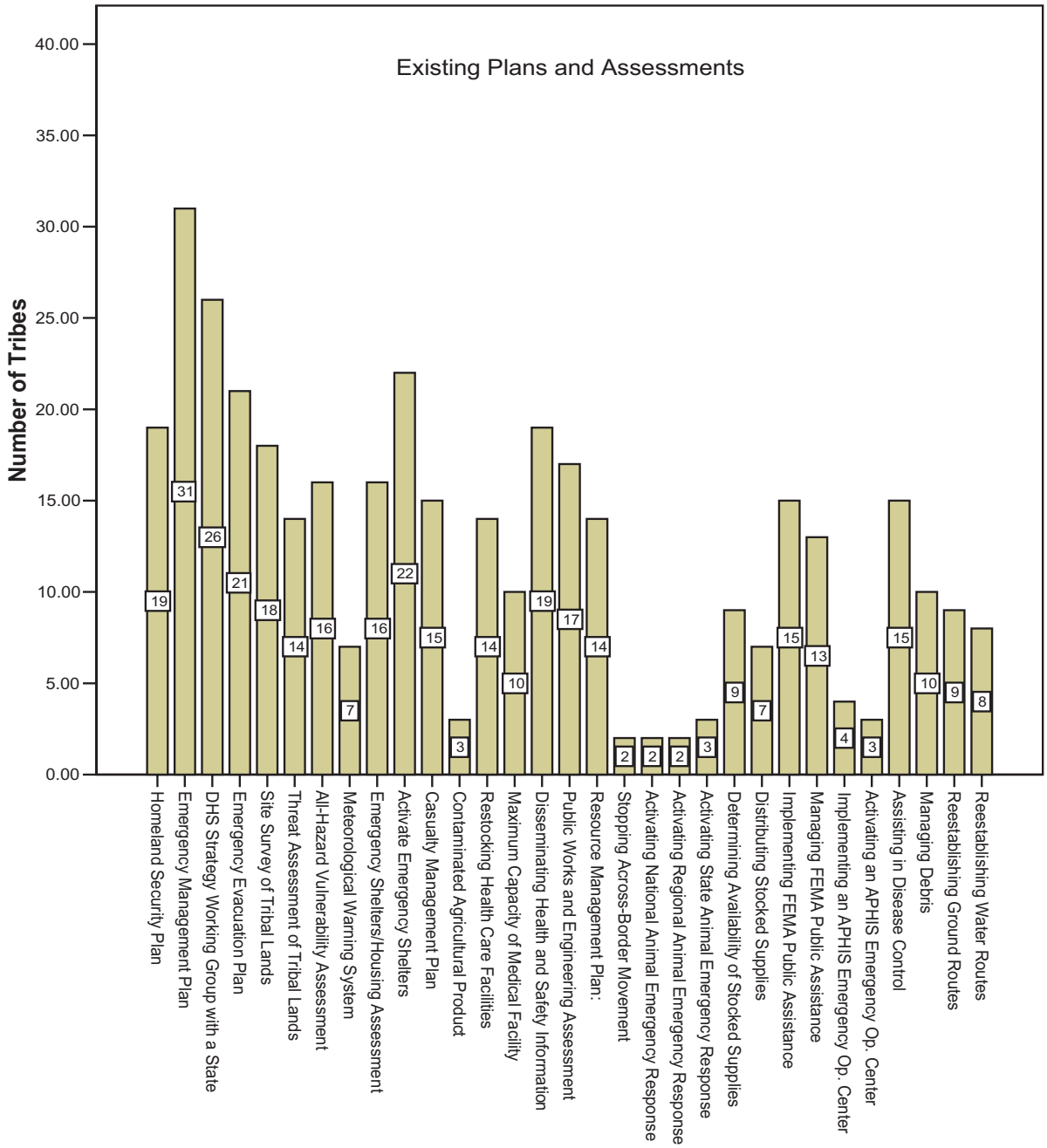
As depicted in Graph 3, a majority of the forty (40) participating Tribes reported that they have a separate homeland security department or emergency management department, coordinator or director.

2. Planning.

The planning preparedness border security baseline which the information shared by the participating border Tribes reveals is a baseline for comparison concerning certain existing plans and assessments of the border Tribes. With regard to this baseline, the forty (40) participating Tribes were surveyed concerning their respective plans and assessments. The specific plans and assessments included in the survey were the following: homeland security plan, emergency management plan, DHS strategy working group with a State, emergency evacuation plan, site survey assessment of tribal lands, threat assessment of tribal lands, all-hazard vulnerability assessment, meteorological warning system, emergency shelters/housing assessment, emergency shelters activation plan, casualty management plan, contaminated agricultural product plan, restocking health care facilities plan, maximum capacity of medical facility assessment, disseminating health and safety information plan, public works and engineering assessment, resource management plan, stopping across-border movement plan, national animal emergency

response activation plan, regional animal emergency response activation plan, state animal emergency response activation plan, stocked supplies availability assessment, stocked supplies distribution plan, FEMA public assistance implementation plan, FEMA public assistance management plan, APHIS emergency operation center implementation plan, APHIS emergency operation center activation plan, disease control assistance plan, debris management plan, ground routes reestablishment plan, and water routes reestablishment plan. Graph 4, below, depicts the number of border Tribes who reported having each plan and having performed each assessment.

Graph 4



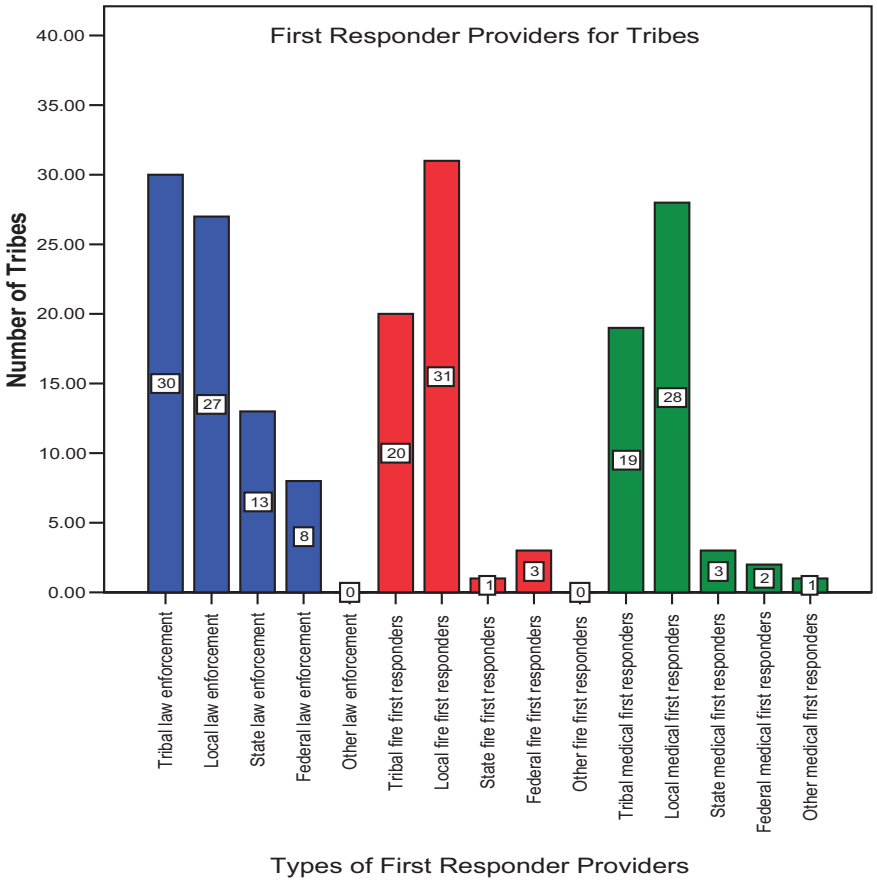
As revealed in Graph 4, the most prevalent existing plan or assessment of the border tribes is an emergency management plan.

3. Resources

The resources preparedness border security baselines which the information shared by the participating border Tribes reveals include the following: (a) A baseline for comparison concerning the first responder providers of the border Tribes;[1] (b) A baseline for comparison concerning the types of incident response equipment possessed by the border Tribes; (c) A baseline for comparison concerning the types of specialized skills and units possessed by the border Tribes; and (d) A baseline for comparison concerning the types of incident response facilities located on the lands of the border Tribes.

With regard to the baseline for comparison concerning the first responder providers of the border Tribes, the forty (40) participating Tribes were surveyed concerning the types of entities providing them with first responder services. The specific entities included in the survey were the following: tribal law enforcement first responders, local law enforcement first responders, state law enforcement first responders, federal law enforcement first responders, other law enforcement first responders, tribal fire first responders, local fire first responders, state fire first responders, federal fire first responders, other fire first responders, tribal emergency medical first responders, local emergency medical first responders, state emergency medical first responders, federal emergency medical first responders, and other emergency medical first responders. Graph 5, below, depicts the types of entities providing first responder services to the border Tribes.

Graph 5

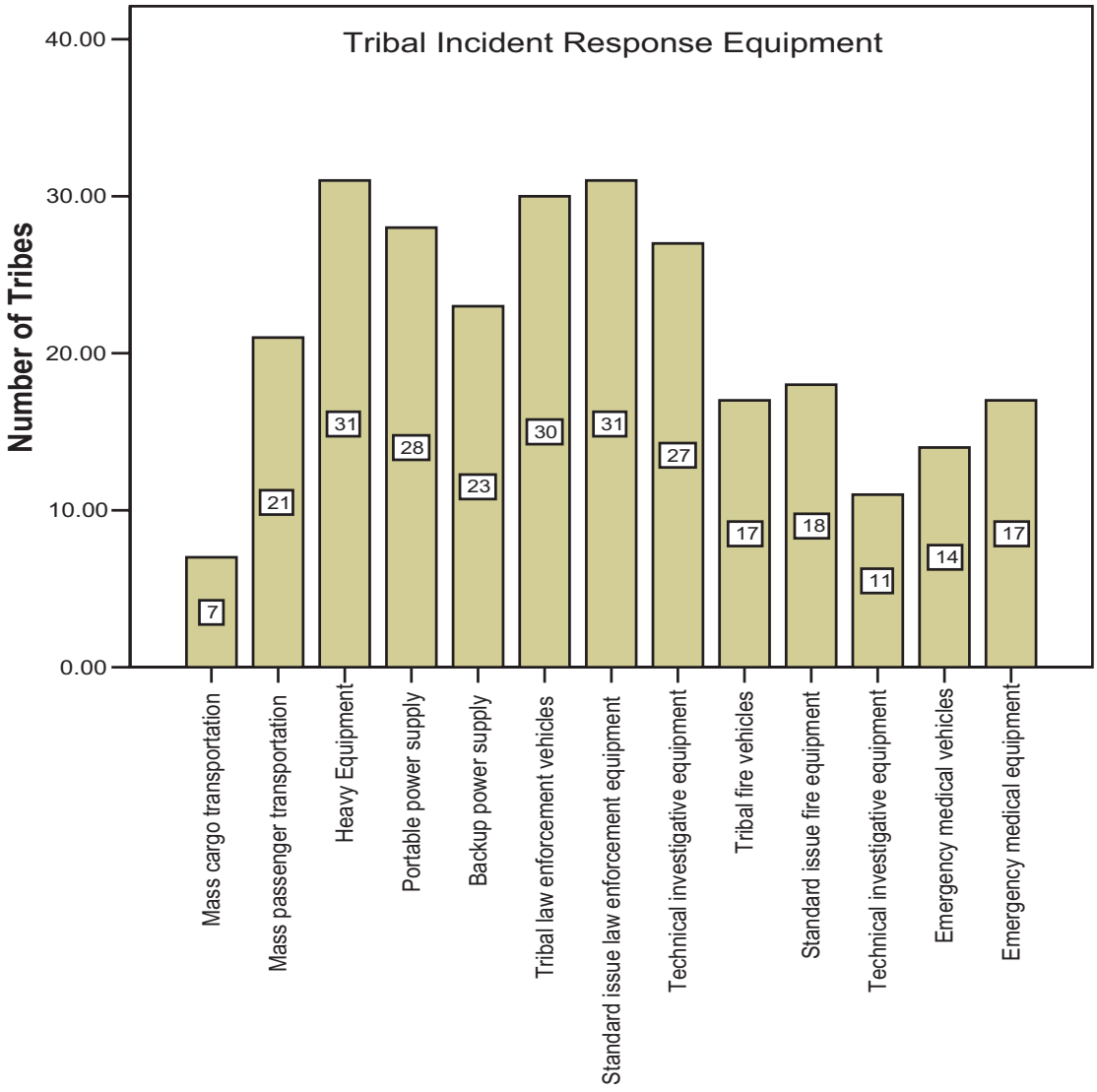


[1] First responders are law enforcement, fire, and emergency medical personnel who first arrive on the scene of an incident and take action to save lives, protect property, and meet basic human needs. First responders may include federal, state, local, or tribal responders.

As depicted in Graph 5, the most prevalent law enforcement first responder providers of the border Tribes are the Tribes themselves; while the most prevalent fire and emergency medical first responder providers of the border Tribes are local entities (i.e., surrounding counties and cities).

With regard to the baseline for comparison concerning the types of incident response equipment possessed by the border Tribes, the forty (40) participating Tribes were surveyed concerning the types of incident response equipment that they each possessed. The types of incident response equipment included in the survey were the following: mass cargo transportation, mass passenger transportation, heavy equipment, portable power supply, backup power supply, tribal law enforcement vehicles, standard issue law enforcement equipment, technical investigative equipment, tribal fire vehicles, standard issue fire equipment, technical investigative equipment, emergency medical vehicles, and emergency medical equipment. Graph 6, below, depicts the types of incident response equipment possessed by the border Tribes.

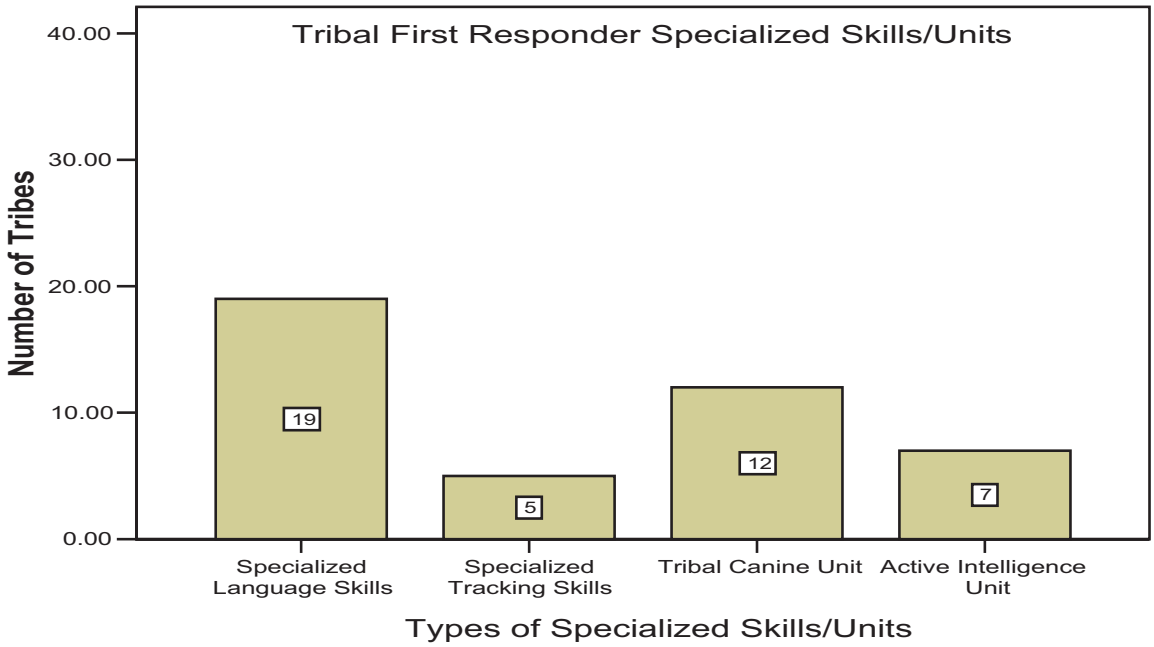
Graph 6



As depicted in Graph 6, the most prevalent types of incident response equipment possessed by the border Tribes are heavy equipment and standard issue law enforcement equipment; while the least prevalent type of incident response equipment possessed by the border Tribes is mass cargo transportation.

With regard to the baseline for comparison concerning the types of specialized skills and units possessed by the border Tribes, the forty (40) participating Tribes were surveyed concerning the specialized skills and units possessed by each Tribe. The specific types of specialized skills and units included in the survey were the following: specialized language skills, specialized tracking skills, tribal canine units, and active intelligence units. Graph 7, below, depicts the types of specialized skills and units possessed by the border Tribes.

Graph 7

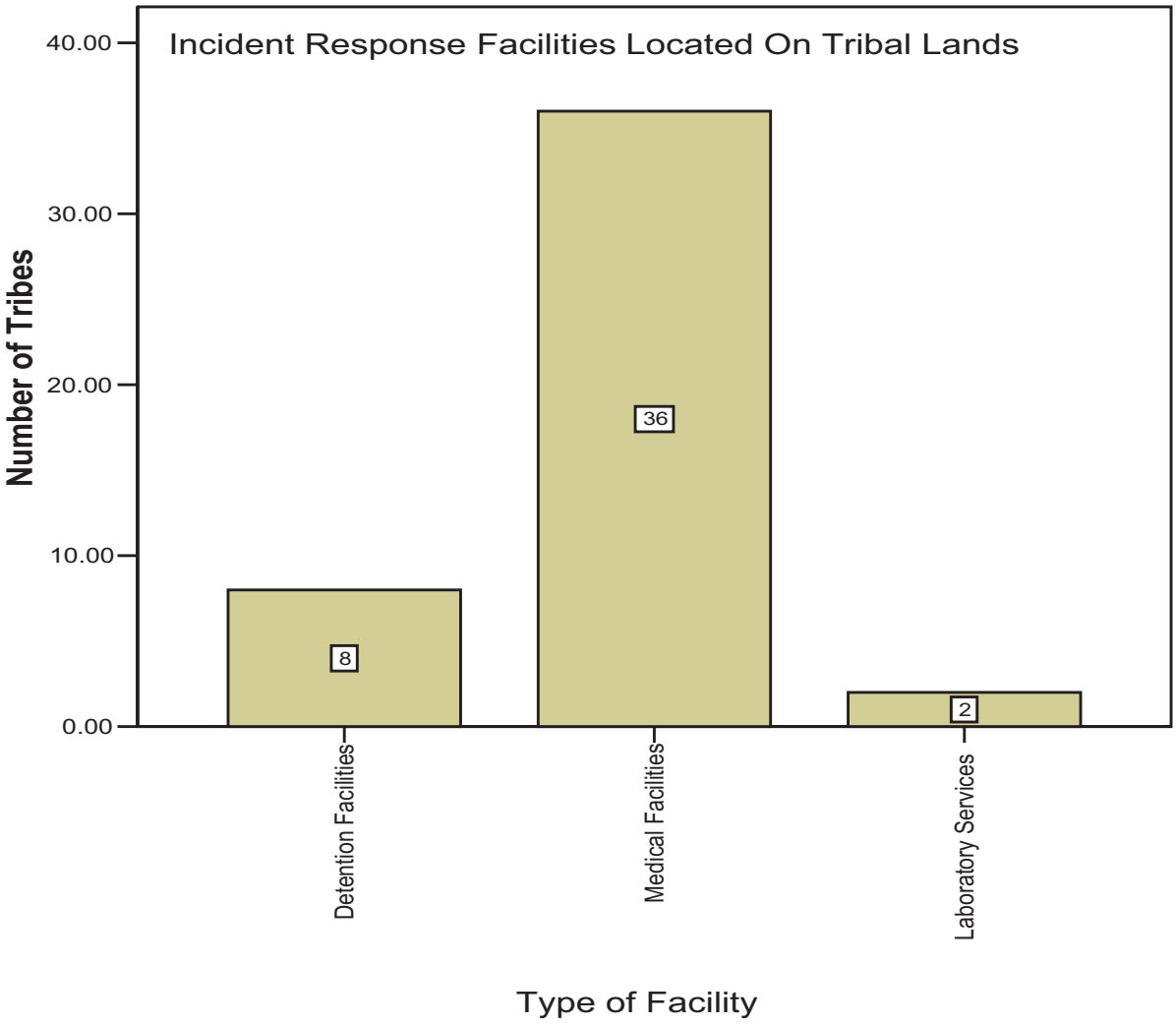


As depicted in Graph 7, the most prevalent types of specialized skills or units possessed by the border Tribes is specialized language skills, while the least prevalent are specialized tracking skills.

With regard to the baseline for comparison concerning the types of incident response facilities located on the lands of the border Tribes, the forty (40) participating border Tribes were surveyed concerning the types of incident response facilities that are located on their respective tribal lands. The specific types of incident response facilities

included in the survey were the following: detention facilities, medical facilities,[1] and forensic laboratory facilities. Graph 8, below, depicts the types of incident response facilities located on the tribal lands of the border Tribes.

Graph 8



As depicted in Graph 8, the most prevalent type of incident response facilities located on the tribal lands of the border Tribes is medical facilities, while the least prevalent is forensic laboratories. It is important to note, though, that of the thirty-six (36) Tribes reporting medical facilities located on their tribal lands, 90% of those facilities are clinics as opposed to hospitals. Moreover, only three (3) of the thirty-six (36) Tribes reported that the medical facilities located on their respective tribal lands had patient beds or were capable to treat emergency trauma.

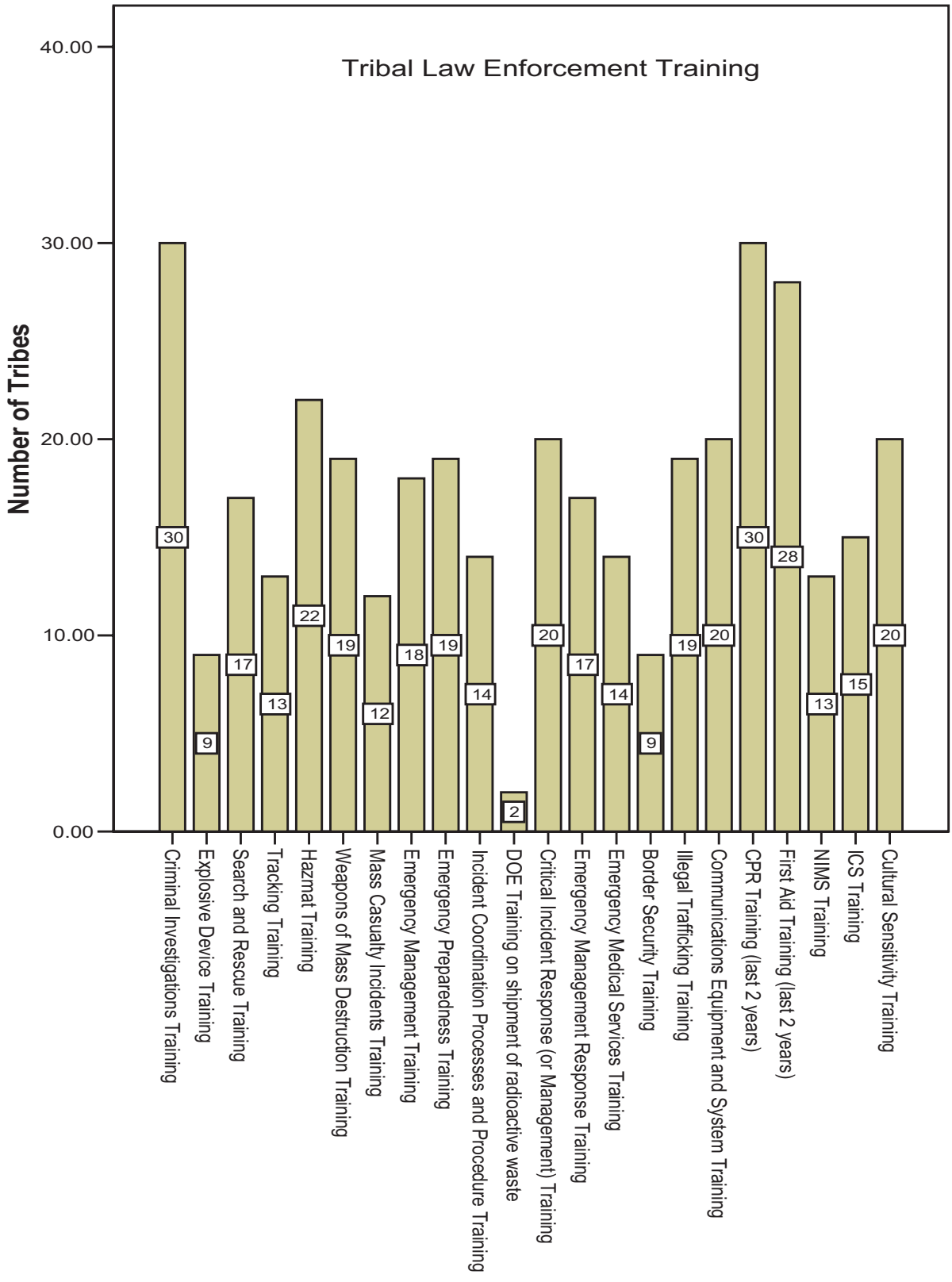
[1] It should be noted that the term "medical facilities" encompasses all types of medical facilities (i.e., clinics and hospitals). Thus, even though a tribe may have a medical facility located on its tribal lands, such does not mean that that facility is capable of rendering adequate medical aid in response to an emergency incident.

4. Training.

The training preparedness border security baselines which the information shared by the participating border Tribes reveals include the following: (a) A baseline for comparison concerning the types of training received by tribal law enforcement first responders; (b) A baseline for comparison concerning the types of training received by tribal fire first responders; (c) A baseline for comparison concerning the types of training received by tribal emergency medical first responders; (d) A baseline for comparison concerning certain meetings that have been attended by tribal first responders; and (e) A baseline for comparison concerning the types of specific scenario training received by tribal first responders.

With regard to the baseline for comparison concerning the types of training received by tribal law enforcement first responders, the forty (40) participating Tribes were surveyed concerning the types of training that their respective tribal law enforcement first responders have received. The specific types of training included in the survey were the following: criminal investigations training, explosive devise training, search and rescue training, tracking training, hazmat training, weapons of mass destruction training, mass casualty incident training, emergency management training, emergency preparedness training, incident coordination processes and procedure training, department of energy training on shipment of radioactive waste, critical incident response or management training, emergency management response training, emergency medical services training, border security training, illegal trafficking training, communications equipment and system training, CPR training (within the last 2 years), first aid training (within the last 2 years), NIMS training, incident command system training, and cultural sensitivity training. Graph 9, page 26, depicts the number of tribes who reported having tribal law enforcement first responders with each type of training.

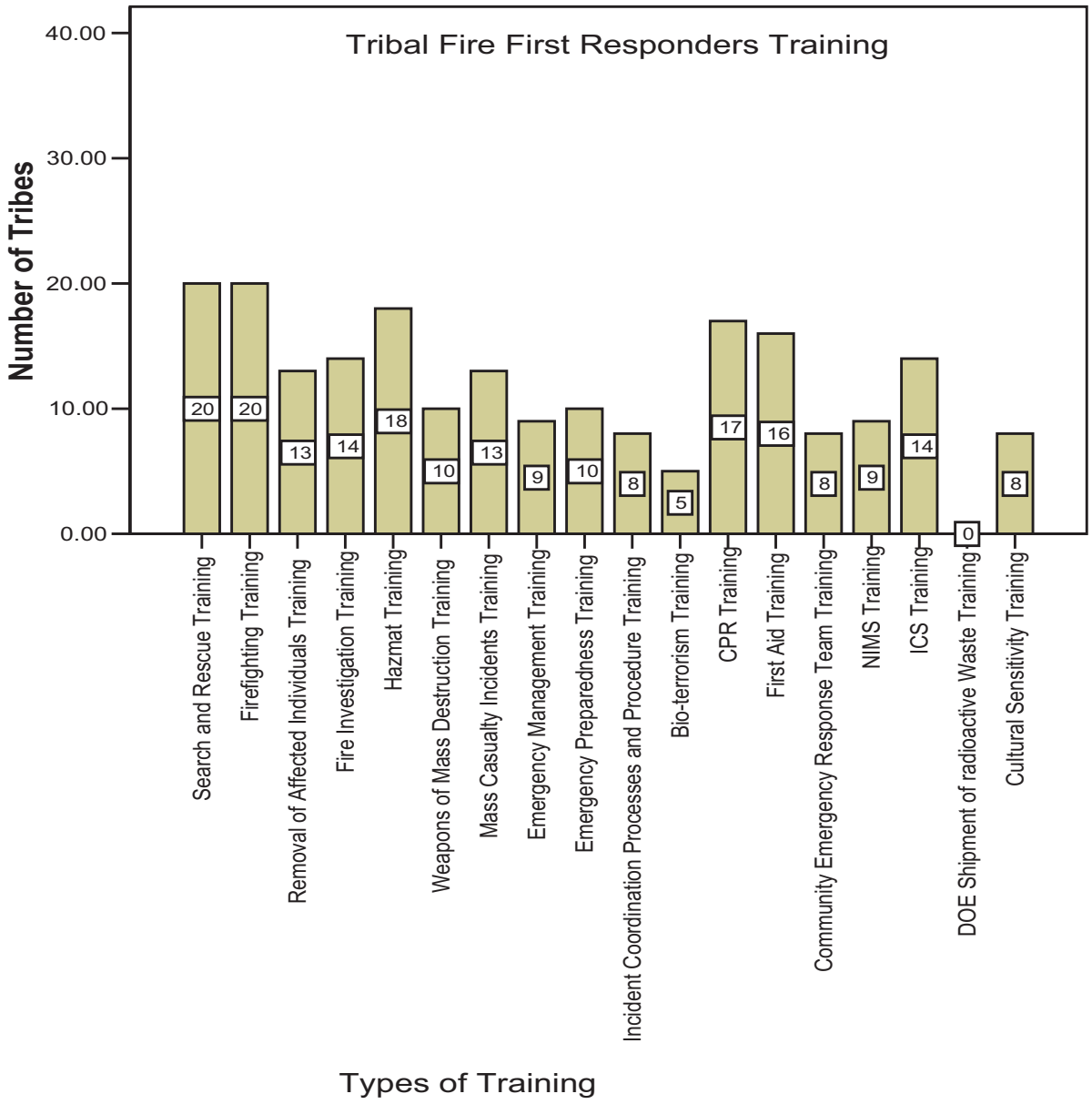
Graph 9



As depicted in Graph 9, the most prevalent types of training received by tribal law enforcement first responders are criminal investigations training and CPR training.

With regard to the baseline for comparison concerning the types of training received by tribal fire first responders, the forty (40) participating Tribes were surveyed concerning the types of training that their respective tribal fire first responders have received. The specific types of training included in the survey were the following: search and rescue training, firefighting training, removal of affected individuals training, fire investigation training, hazmat training, weapons of mass destruction training, mass casualty incident training, emergency management training, emergency preparedness training, incident coordination processes and procedure training, bio-terrorism training, CPR training, first aid training, community emergency response team training, NIMS training, incident command system training, department of energy shipment of radioactive waste training, and cultural sensitivity training. Graph 10, below, depicts the number of tribes who reported having tribal fire first responders with each type of training.

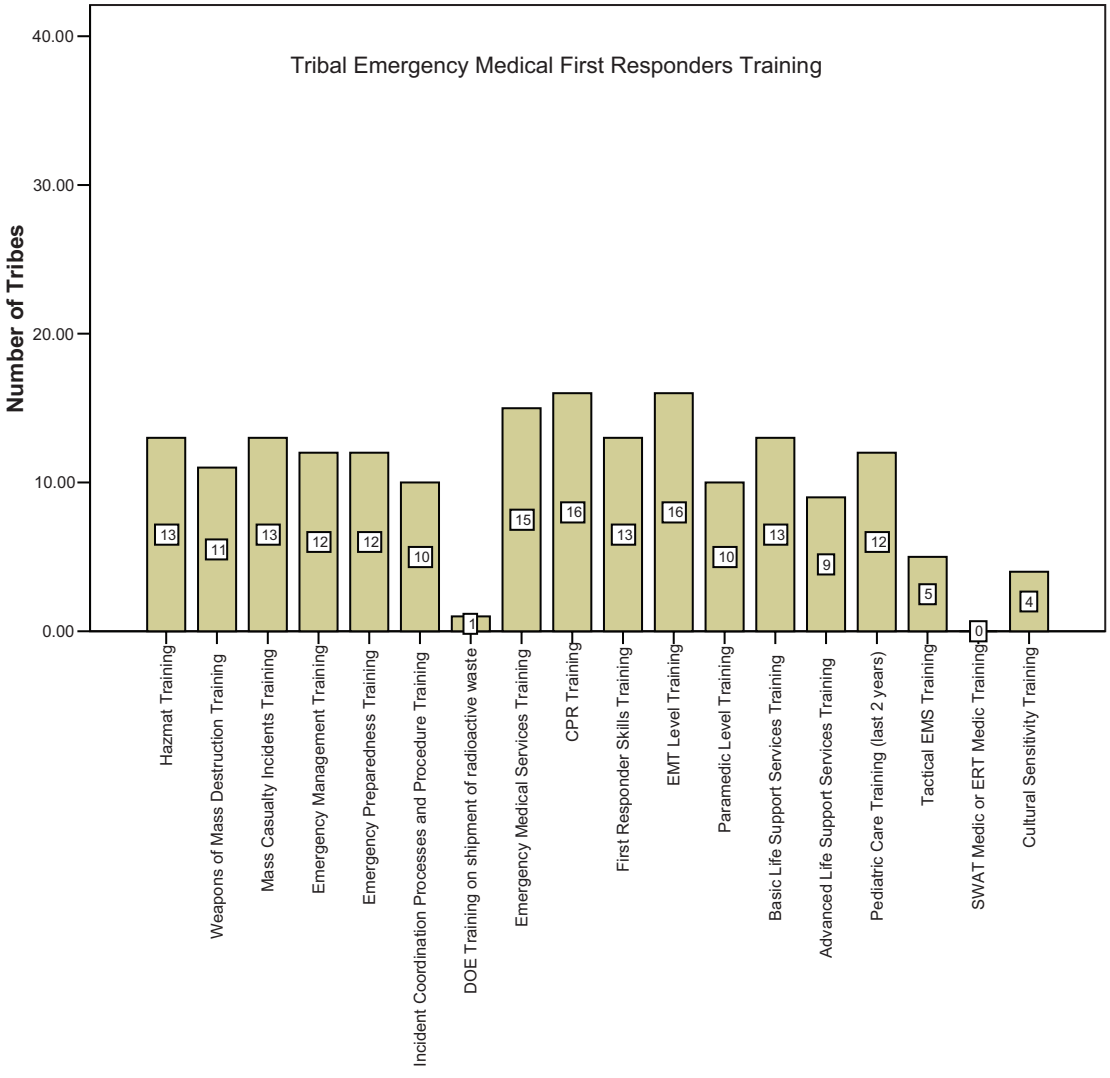
Graph 10



As depicted in Graph 10, the most prevalent types of training received by tribal fire first responders are search and rescue training and firefighting training.

With regard to the baseline for comparison concerning the types of training received by tribal emergency medical first responders, the forty (40) participating Tribes were surveyed concerning the types of training that their respective tribal emergency medical first responders have received. The specific types of training included in the survey were the following: hazmat training, weapons of mass destruction training, mass casualty incidents training, emergency management training, emergency preparedness training, incident coordination processes and procedure training, department of energy training on the shipment of radioactive waste, emergency medical services training, CPR training, first responder skills training, EMT level training, paramedic level training, basic life support services training, advanced life support services training, pediatric care training (within the last two years), tactical EMS training, SWAT medic or ERT medic training, and cultural sensitivity training. Graph 11, below, depicts the number of tribes who reported having tribal emergency medical first responders with each type of training.

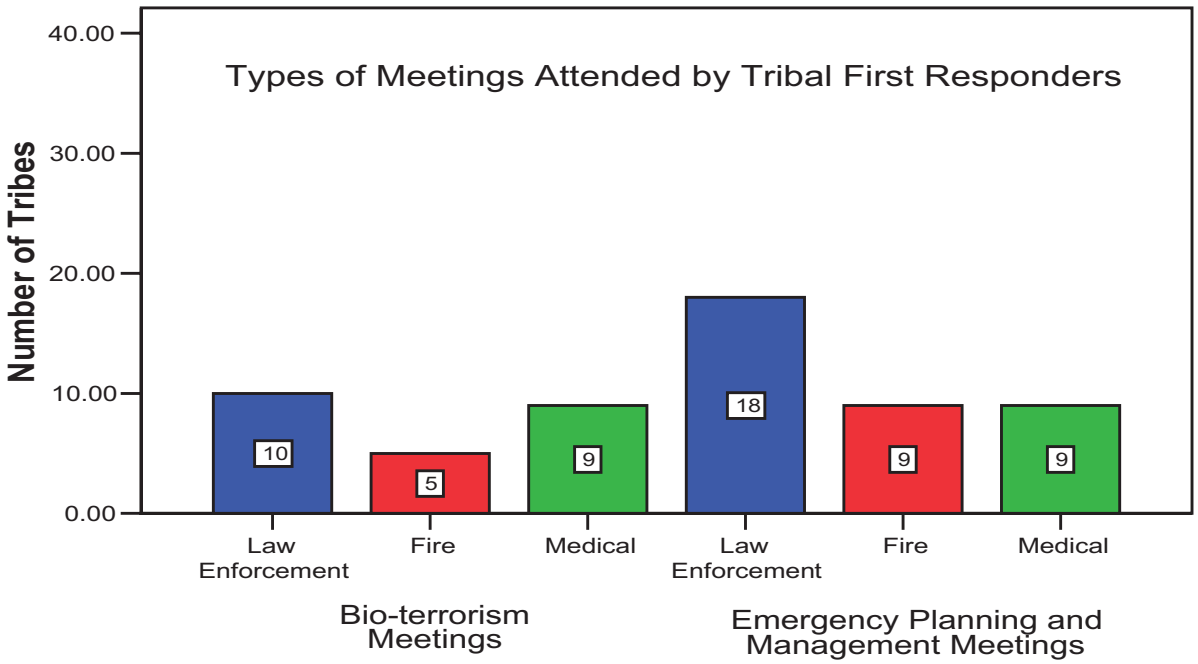
Graph 11



As depicted in Graph 11, the most prevalent types of training received by tribal emergency medical first responders are CPR training and EMT level training.

With regard to the baseline for comparison concerning certain meetings that have been attended by tribal first responders, the forty (40) participating Tribes were surveyed concerning whether their law enforcement, fire, and emergency medical first responders had attended bio-terrorism meetings, and/or emergency planning and management meetings. Graph 12, below, depicts the number of Tribes who reported that their tribal first responders had attended each type of meeting.

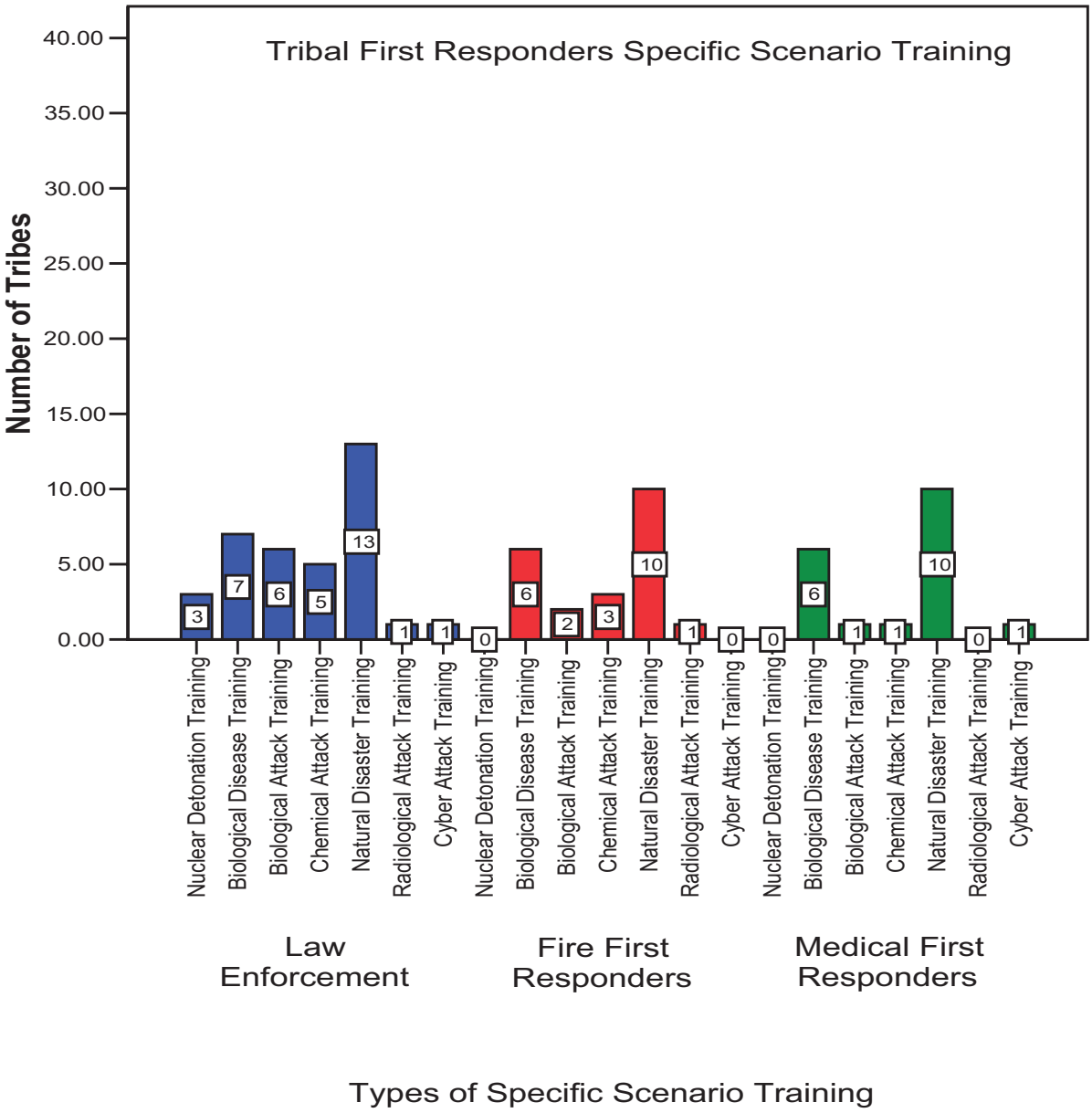
Graph 12



As depicted in Graph 12, the most common types of meetings attended by tribal first responders are emergency planning and management meetings attended by tribal law enforcement first responders.

With regard to the baseline for comparison concerning the types of specific scenario training received by tribal first responders, the forty (40) participating tribes were surveyed on the types of specific scenario training that their respective tribal first responders (law enforcement, fire, and emergency medical) have received. The types of specific scenario training included in the survey were the following: nuclear detonation training, biological disease training, biological attack training, chemical attack training, natural disaster training, radiological attack training, and cyber attack training. Graph 13, page 30, depicts the number of tribes who reported having first responders with each type of specific scenario training.

Graph 13



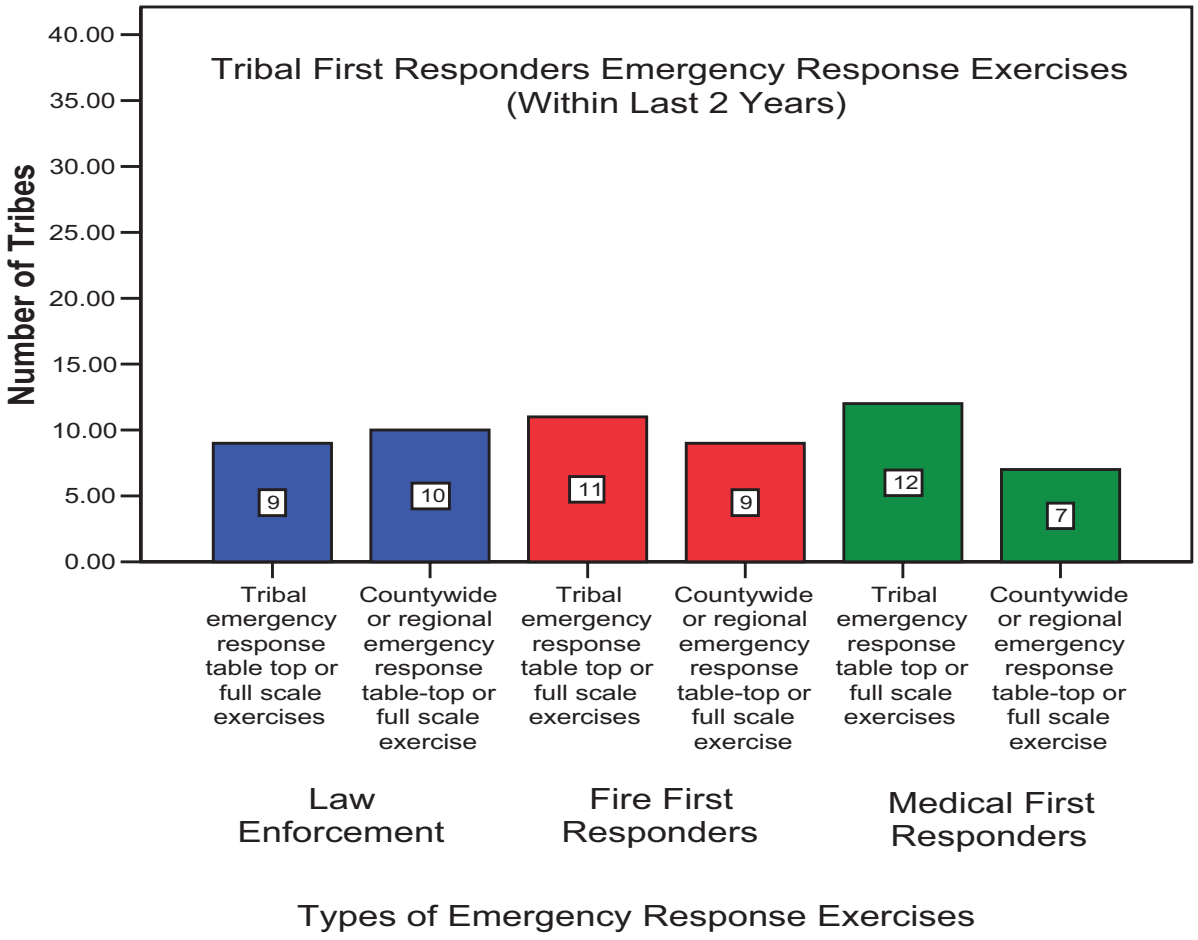
As depicted in Graph 13, the most prevalent specific scenario training received by tribal first responders is natural disaster training.

5. Exercises.

The exercises preparedness border security baseline which the information shared by the participating border Tribes reveals is a baseline for comparison concerning the emergency response exercises that the Tribes respective tribal first responders have participated within the last two (2) years. More particularly, the border Tribes were surveyed concerning certain types of emergency response exercises that their respective tribal first responders (law enforcement, fire, and emergency medical) have participated in the last two (2) years. The types of emergency response exercises included in the survey were the following: tribal emergency response table top or full scale exercises,

and countywide or regional emergency response table-top or full scale exercise. Graph 14, below, depicts the number of border Tribes who reported having tribal first responders who have participated in each type of emergency response exercise.

Graph 14



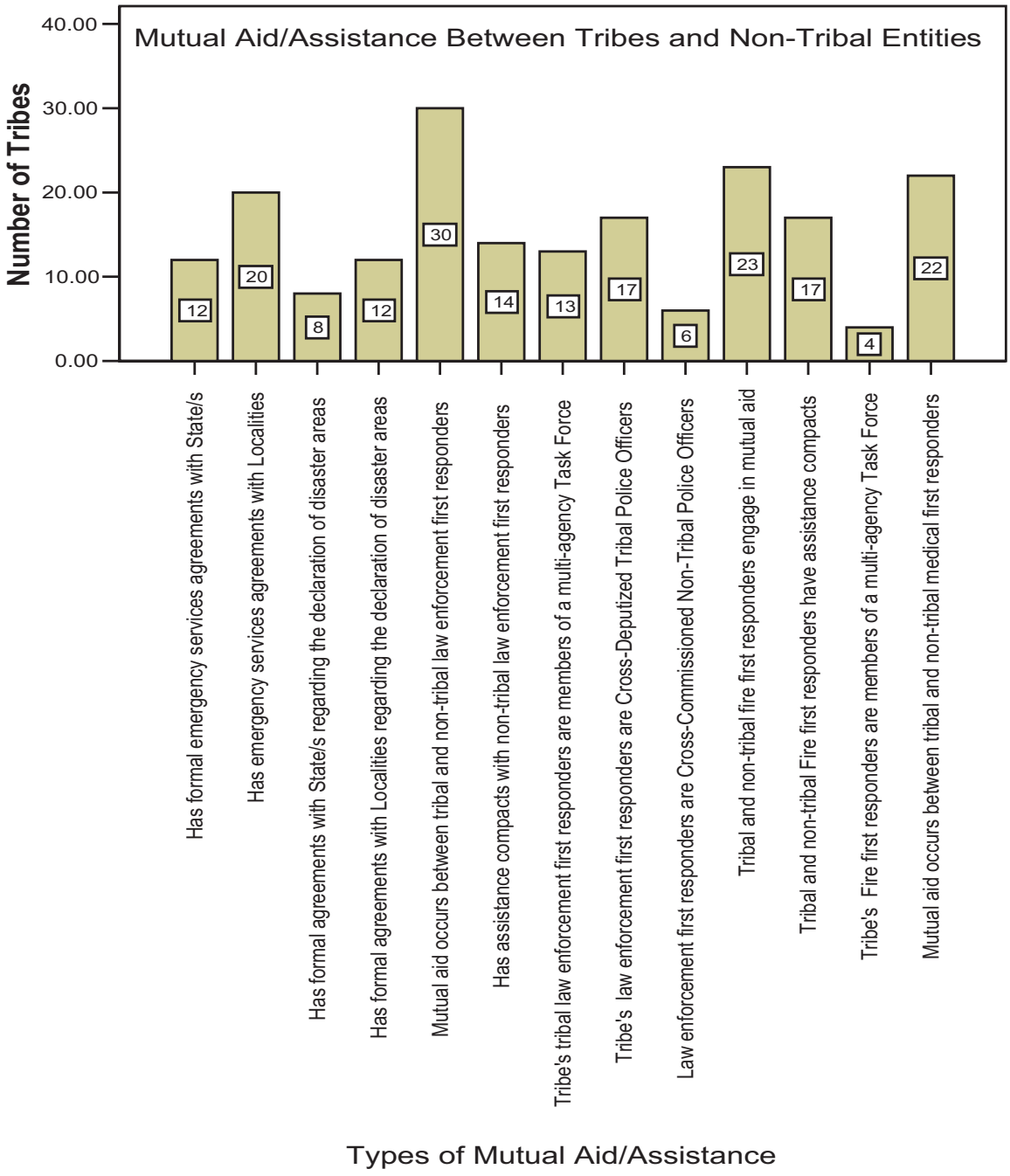
As depicted in Graph 14, the most prevalent emergency response exercises in which tribal law enforcement first responders have participated are the countywide or regional emergency response table-top or full scale exercises; whereas the most prevalent emergency response exercises in which tribal fire and emergency medical first responders have participated are the tribal emergency response table-top or full scale exercises.

6. Mutual Aid and Assistance Compacts.

The mutual aid and assistance compacts preparedness border security baseline which the information shared by the participating border Tribes reveals is a baseline for comparison concerning the types of mutual aid and assistance compacts in existence between the border Tribes and non-tribal entities. The types of mutual aid and assistance compacts included in the survey include the following: formal emergency services agreements with states or localities, formal agreements regarding the declaration of disaster

areas with states or localities, mutual aid between tribal and non-tribal law enforcement first responders, mutual aid between tribal and non-tribal fire first responders, mutual aid between tribal and non-tribal emergency medical first responders, assistance compacts with non-tribal law enforcement or fire first responders, multi-agency law enforcement or fire task force membership, cross-deputization, and cross-commissions. Graph 15, below, depicts the types of mutual aid and assistance compacts in existence between the border Tribes and non-tribal entities.

Graph 15



As depicted in Graph 15, the most prevalent types of mutual aid or assistance compacts are mutual aid between tribal and non-tribal first responders.

B. Tribal Border Security Preparedness Best Practices.

The information shared by the participating Tribes in the TBS Pilot Program reveals a number of tribal border security best practices with regard to the Preparedness function. Those best practices pertain to preparedness with regard to organization and leadership, planning, resources, training, exercises, and mutual aid and assistance compacts. These best practices are each summarized in turn.

1. Organization and Leadership.

The organization and leadership preparedness border security best practice which the information shared by the participating border Tribes reveals pertains to those Tribes that have a specifically designated homeland security department, director, or coordinator.

2. Planning.

There are a number of planning preparedness border security best practices which the information shared by the participating border Tribes reveals. One best practice pertains to those Tribes who have participated in a DHS strategy working group with a State. A second best practice pertains to those Tribes who have a homeland security plan. A third best practice pertains to those Tribes with homeland security plans that specifically address border security, critical infrastructure, and interoperable communications, among other things. A fourth best practice pertains to those Tribes with emergency management plans that specifically address first responders (law enforcement, fire and emergency medical), border security, protection of critical infrastructure, and interoperable communications, among other things.

3. Resources.

There are a number of resources preparedness border security best practices which the information shared by the participating border Tribes reveals. One best practice pertains to those Tribes with capabilities to provide their own first responder services. A second best practice pertains to those Tribes who have entered into first responder agreements with non-tribal entities (i.e., federal, state, local, or other entities). A third best practice pertains to those Tribes with any of the specialized skills or units contained in the survey.

4. Training.

There are a number of training preparedness border security best practices which the information shared by the participating border Tribes reveals. One best practice pertains to those Tribes with tribal law enforcement first responders who have received any of the types of training included in the survey. A second best practice pertains to those Tribes with tribal law enforcement first responders who have received border security training, illegal trafficking training, and tracking training, among other training. A third best practice pertains to those Tribes with tribal fire first responders who have received any of the types of training included in the survey. A fourth best practice pertains to those Tribes with tribal emergency medical first responders who have received any of the types of training included in the survey. A fifth best practice pertains to those Tribes who have tribal first responders who have attended bio-terrorism meetings, and emergency planning and management meetings. A sixth best practice pertains to those Tribes with tribal first

responders (law enforcement, fire, and/or emergency medical) who have received any of the types of specific scenario training included in the survey.

5. Exercises.

The exercises preparedness border security best practice which the information shared by the participating border Tribes reveals pertains to those Tribes with tribal first responders who have participated in any emergency response exercise within the last two (2) years. Of those Tribes, particular kudos goes to the Tribes with tribal first responders who have participated in countywide or regional emergency response exercises given the Department of Homeland Security's present emphasis on regionalization.

6. Mutual Aid and Assistance Compacts.

There are a number of mutual aid and assistance compacts preparedness border security best practices which the information shared by the participating border Tribes reveals. One border security best practice is that all of the participating border Tribes with tribal law enforcement first responders reported mutual aid occurring between them and non-tribal law enforcement first responders. A second border security best practice is that all of the participating border Tribes with tribal fire first responders reported mutual aid occurring between them and non-tribal fire first responders. A third border security best practice is that all of the participating border Tribes with tribal emergency medical first responders reported mutual aid occurring between them and non-tribal emergency medical first responders. A fourth border security best practice pertains to those participating border Tribes who have achieved any of the types of mutual aid and assistance compacts identified in the survey.

C. Tribal Border Security Preparedness Alerts.

The information shared by the participating Tribes in the TBS Pilot Program reveals a number of tribal border security alerts with regard to the Preparedness function. Those alerts pertain to preparedness with regard to organization and leadership, planning, resources, training, exercises, and mutual aid and assistance compacts. These alerts are each summarized in turn.

1. Organization and Leadership.

The organization and leadership preparedness border security alert which the information shared by the participating border Tribes reveals is that some tribes have not yet designated a separate homeland security or emergency management department, director, or coordinator.

2. Planning.

There are several planning preparedness border security alerts which the information shared by the participating border Tribes reveals. One border security alert is that of the thirty-one (31) types of plans and assessments about which the border Tribes were surveyed, only four (4) of said plans and assessments have been achieved by 50% or more of the participating border Tribes. A second border security alert is that more than half of the participating border Tribes reported not having a homeland security plan. A third

border security alert is that of the homeland security plans of the participating Tribes, 57.9% of said plans do not specifically address border security, 26.3% of said plans do not specifically address protection of critical infrastructure, and 26.3% of said plans do not specifically address interoperable communications. A fourth border security alert is that of the emergency management plans of the participating Tribes, 75.2% of said plans do not specifically address border security, 45.2% of said plans do not specifically address protection of critical infrastructure, and 32.3% of said plans do not specifically address interoperable communications.

3. Resources.

There are several resources preparedness border security alerts which the information shared by the participating border Tribes reveals. One border security alert is that ten (10) of the participating border Tribes reported that they do not have their own tribal law enforcement first responders, twenty (20) of the participating border Tribes reported that they do not have their own tribal fire first responders, and twenty (20) of the participating border Tribes reported that they do not have their own tribal emergency medical first responders. A second border security alert is that collectively the participating border Tribes reported that they needed at least five hundred and thirty-three (533) additional tribal law enforcement officers. A third border security alert is that only eleven (11) of the forty (40) participating border Tribes reported that they possess some technical investigative equipment. A fourth border security alert is that only seven (7) of the forty (40) participating border Tribes reported that they have an active intelligence unit. A fifth border security alert is that only eight (8) of the participating border Tribes reported that there were detention facilities located on their respective tribal lands. A sixth border security alert is that only 7.5% of the participating border Tribes have medical facilities located on their tribal lands that have patient beds or that are capable of treating emergency trauma.

4. Training.

There are several training preparedness border security alerts which the information shared by the participating border Tribes reveals. One border security alert is that ten (10) or more of the thirty (30) participating Tribes with tribal law enforcement first responders reported that their tribal law enforcement first responders did not have the following types of training: explosive devise training, search and rescue training, tracking training, weapons of mass destruction training, mass casualty incident training, emergency management training, emergency preparedness training, incident coordination processes and procedure training, department of energy training on shipment of radioactive waste, critical incident response or management training, emergency management response training, emergency medical services training, border security training, illegal trafficking training, communications equipment and system training, NIMS training, incident command system training, and cultural sensitivity training. A second border security alert is that only nine (9) of the participating border Tribes reported having tribal law enforcement first responders with border security training. A third border security alert is that seventeen (17) or more of the thirty (30) participating Tribes with tribal law enforcement first responders reported that their tribal law enforcement first responders did not have the following types of specific scenario training: nuclear detonation training, biological disease training, biological

attack training, chemical attack training, natural disaster training, radiological attack training, and cyber attack training. A fourth border security alert is that ten (10) or more of the twenty (20) participating Tribes with tribal fire first responders reported that their tribal fire first responders did not have the following types of training: weapons of mass destruction training, emergency management training, emergency preparedness training, incident coordination processes and procedure training, bio-terrorism training, community emergency response team training, NIMS training, department of energy shipment of radioactive waste training, and cultural sensitivity training. A fifth border security alert is that ten (10) or more of the twenty (20) participating Tribes with tribal fire first responders reported that their tribal fire first responders did not have the following types of specific scenario training: nuclear detonation training, biological disease training, biological attack training, chemical attack training, natural disaster training, radiological attack training, and cyber attack training. A sixth border security alert is that ten (10) or more of the nineteen (19) participating Tribes with tribal emergency medical first responders reported that their tribal emergency medical first responders did not have the following types of training: tactical EMS training, SWAT medic or ERT medic training, and cultural sensitivity training. A seventh border security alert is that (nine) 9 or more of the nineteen (19) participating Tribes with tribal emergency medical first responders reported that their tribal emergency medical first responders did not have the following types of specific scenario training: nuclear detonation training, biological disease training, biological attack training, chemical attack training, natural disaster training, radiological attack training, and cyber attack training.

5. Exercises.

The exercises preparedness border security alert which the information shared by the participating border Tribes reveals is that less than half of the participating border Tribes with tribal first responders have participated in countywide or regional emergency response exercises within the last two (2) years.

6. Mutual Aid and Assistance Compacts.

The mutual aid and assistance compacts preparedness border security alert which the information shared by the participating border Tribes reveals is that twenty (20) or more of the participating Tribes reported that they do not currently have formal emergency services agreements with states or localities, formal agreements regarding the declaration of disaster areas with states or localities, multi-agency task force membership with non-tribal entities, and cross-deputized or cross-commissioned law enforcement officers.

Border Security In Terms Of The National Preparedness Goal: Communications and Information Management -- Interoperable Communications

Communications and Information Management is a function that falls within the Department of Homeland Security's common target tasks and capabilities, and therefore, is relevant in assessing border security in terms of the evolving Target Capabilities List.[1] A key to Communications and Information Management is that interoperable communications processes, procedures, and systems exist across all agencies and

[1] *See Target Capabilities List: Version 1.1*, U.S. Department of Homeland Security, May 23, 2005, p. 12.

jurisdictions.[1] Interoperable Communications is described as the "capability to provide uninterrupted flow of critical information among responding multi-disciplinary and multi-jurisdictional agencies at all levels of government."[2] The desired outcome is that a "continuous flow of critical information is maintained among emergency responders, command posts, agencies, and government officials for the duration of the emergency response operation."[3]

In the TBS Pilot Program, the forty (40) participating Tribes shared information pertaining to their respective interoperable communications processes, procedures, and systems. The information shared, when analyzed in the aggregate, reveals certain tribal border security baselines, best practices, and alerts relevant to the Communications and Information Management function. These baselines, best practices, and alerts are each summarized in turn.

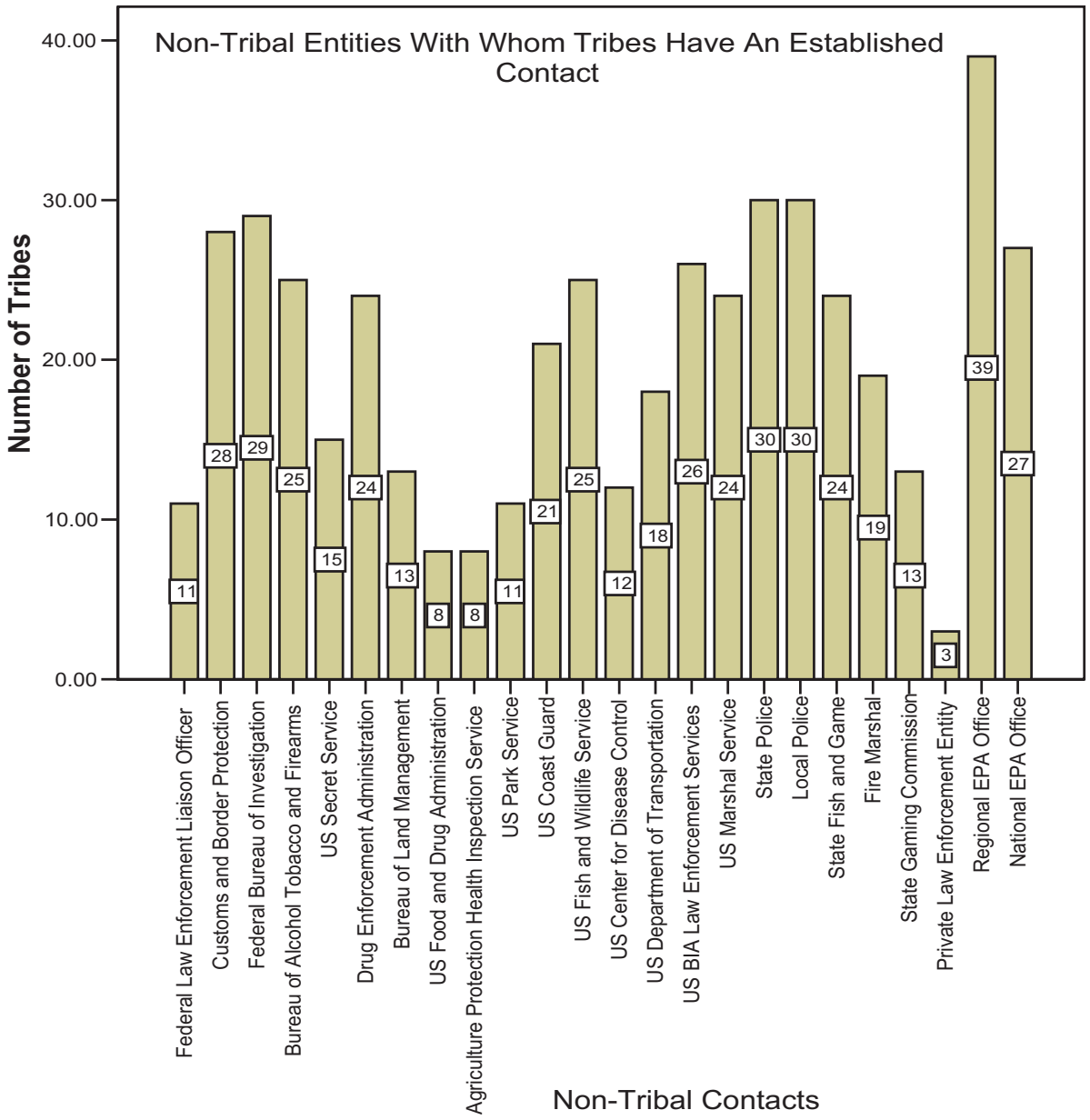
A. Tribal Border Security Interoperable Communications Baselines.

The information shared by the participating Tribes in the TBS Pilot Program reveals a number of tribal border security baselines with regard to the Communications and Information Management function. Four such baselines include: (a) A baseline for comparison of border Tribes' established non-tribal contacts; (b) A baseline for comparison of border Tribes' communications equipment capabilities; (c) A baseline for comparison of entities with whom some communications interoperability has been achieved by border Tribes; and (d) A baseline for comparison of border Tribes' obstacles to communications interoperability.

With regard to the baseline for comparison of border Tribe's established non-tribal contacts, the forty (40) participating Tribes were surveyed concerning certain federal, state, local, and private entities with whom each Tribe may have an established contact. The specific non-tribal entities included in the survey were the following: the Environmental Protection Agency (national and regional offices), private law enforcement, State gaming commissions, fire marshals, State fish and game, local police, State police, U.S. Marshal Service, U.S. BIA Law Enforcement Services, U.S. Department of Transportation, U.S. Center for Disease Control, U.S. Fish and Wildlife Service, U.S. Coast Guard, U.S. Park Service, Agriculture Protection Health Inspection Service, U.S. Food and Drug Administration, Bureau of Land Management, Drug Enforcement Administration, U.S. Secret Service, Bureau of Alcohol Tobacco and Firearms, Federal Bureau of Investigation, Customs and Border Protection, and Federal Law Enforcement Liaison Officer. Graph 16, page 38, depicts the number of border Tribes who reported an established contact with each of these non-tribal entities.

[1] *Id.*
[2] *Id.* at 17.
[3] *Id.*

Graph 16

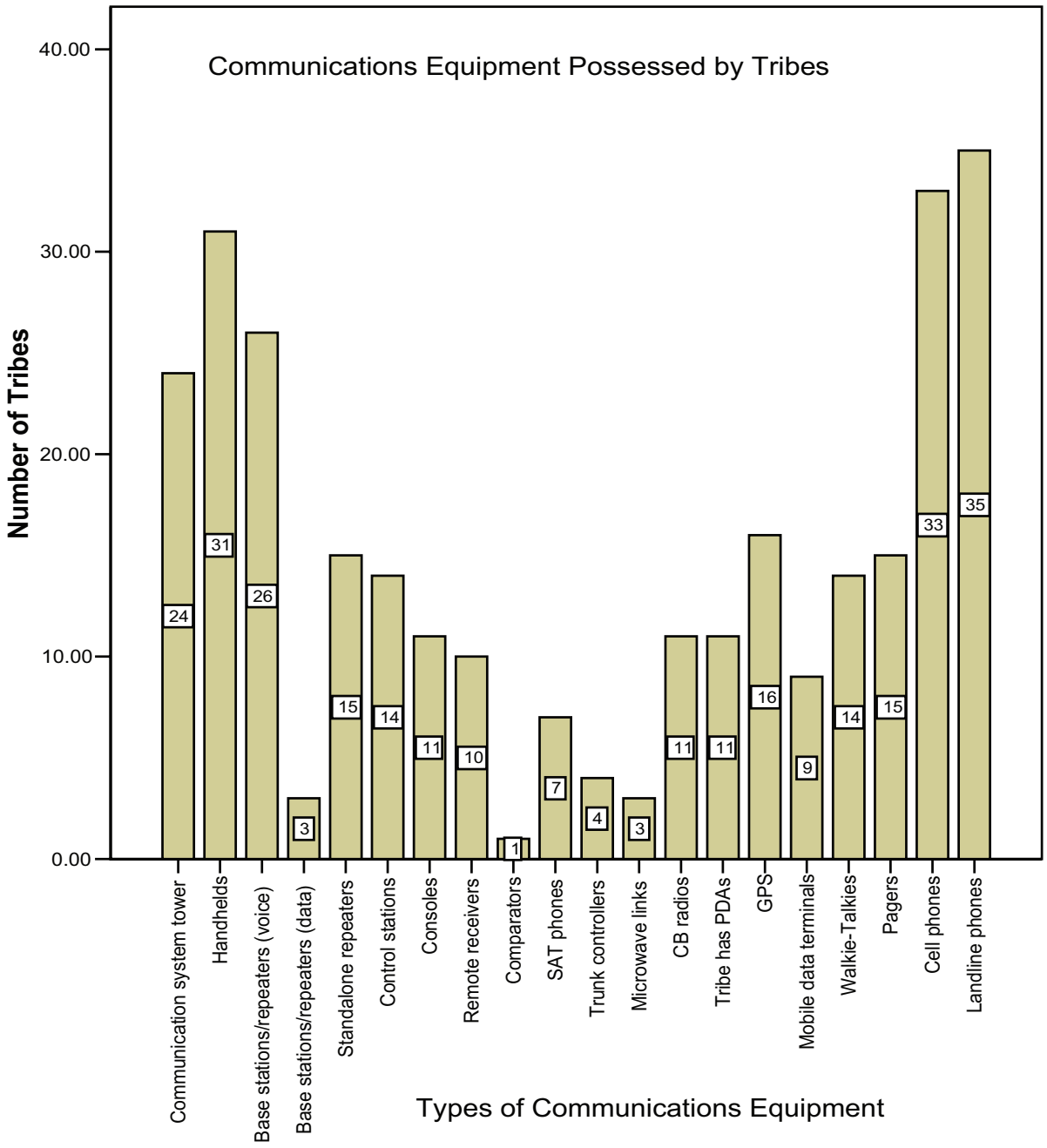


As revealed in Graph 16, the most prevalent established non-tribal entity contacts exist between the border Tribes and the regional Environmental Protection Agency offices. The least prevalent established non-tribal entity contacts is between the border Tribes and private law enforcement entities.

With regard to the baseline for comparison of border Tribes' communications equipment capabilities, the forty (40) participating Tribes were surveyed concerning the communications equipment that they each possess. The specific communications equipment included in the survey included: communication system towers, handhelds,[1] base stations/repeaters (voice),[2] base stations/repeaters (data),[3] standalone repeaters,[4] control stations,[5] consoles,[6] remote receivers,[7] comparators,[8] satellite phones, trunk controllers,[9] microwave links,[10] CB radios, PDAs,[11] GPS devices,[12] mobile data terminals,[13] walkie-talkies, pagers, cell phones, and landline phones. Graph 17, page 40, depicts the number of border Tribes reporting possession of each type of communications equipment.

[1] A handheld is a device that is portable and used for wireless communications.
[2] A base station/repeater (voice) is a station or other communication center that increases the area of wireless voice communication coverage.
[3] A base station/repeater (data) is a station or other communication center that increases the area of wireless data communication coverage.
[4] A standalone repeater is a communication site that supplements a network by giving back-up support in case the primary communication site fails. They can also provide interoperability between agencies who are on different networks.
[5] A control station is a station that enables an entire system to work off a single compact base by integrating telephone and radio service through most business telephone systems.
[6] A console is a self contained radio dispatching unit that controls single or multiple base stations. Multiple consoles can be used to access and control a radio system.
[7] A remote receiver is a communication receiver that operates from a distance from the main communication station or site. It can be used to receive information at a distant site from the main communication station or site.
[8] A comparator processes data collected from multiple receivers to create the best possible transmission signal.
[9] A trunk controller is a controller used to manage a large number of users on a relatively small number of communication paths.
[10] A microwave link is a point to point link that provides voice and data services between the two points when a wired connection (i.e., coaxial cable or fiber-optic connection) is not available (i.e., because of practical or financial reasons).
[11] A personal data assistant ("PDA") is an electronic device (usually handheld) that stores and transmits data (i.e., Blackberry or TREO).
[12] A global positioning system ("GPS") is an electronic device (can be handheld) used to navigate.
[13] A mobile data terminal is a moveable wireless computing device used to send and receive information over a wireless data network.

Graph 17



As revealed in Graph 17, the most common communications equipment possessed by the border Tribes is landline phones.[1] The least common communications equipment possessed by the border Tribes is comparators.[2]

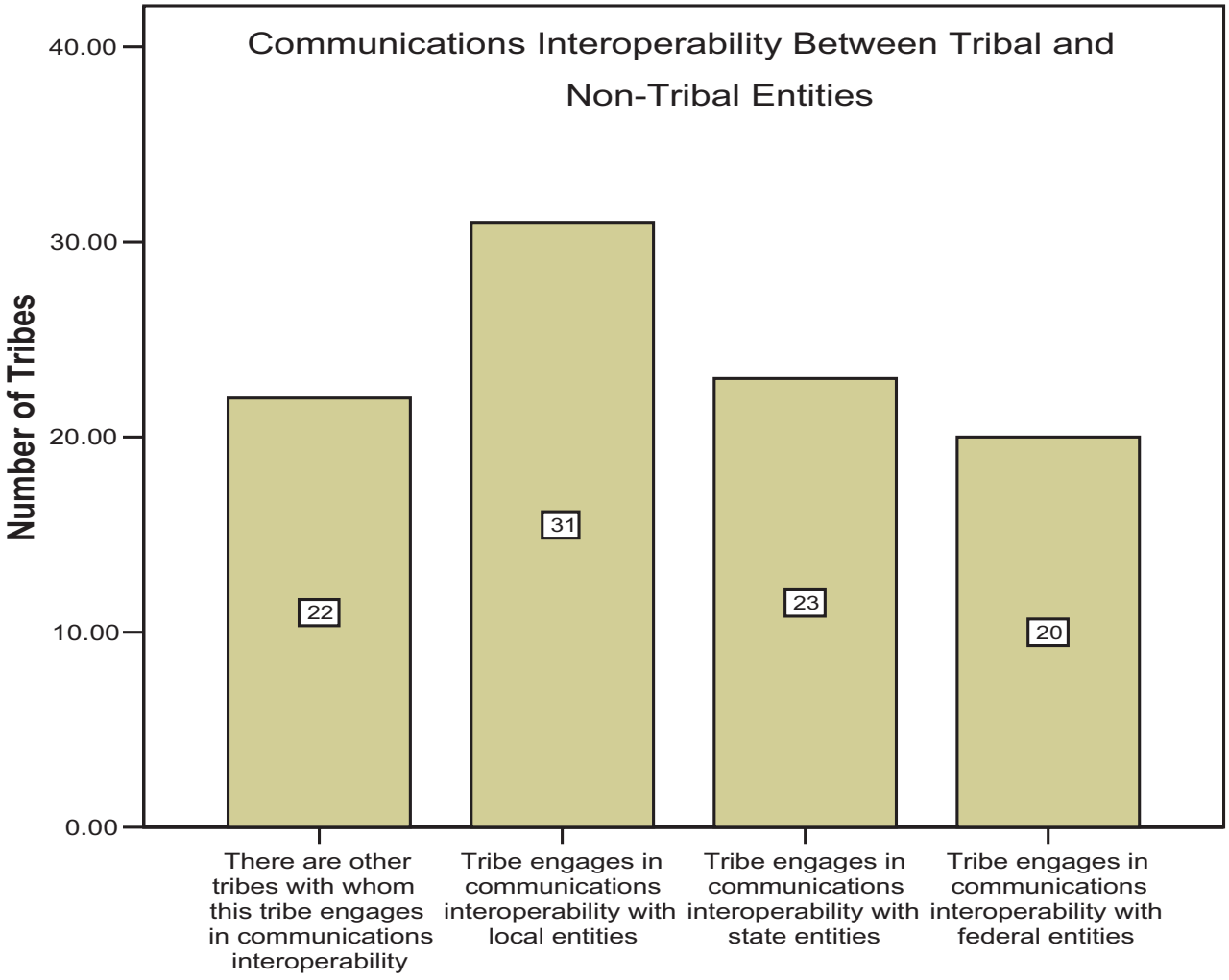
With regard to the baseline for comparison of entities with whom some communications interoperability has been achieved by border Tribes, the forty (40)

[1] Graph 17 reveals that thirty-five (35) of the forty (40) participating Tribes have communications systems that include landline phones. The other five (5) participating Tribes have landline phones but reported that they do not have a communications system. Thus, Graph 17 pertains to the participating Tribes with communications systems and with landline phones that comprise each system.

[2] *See* Footnote # 69, *supra*.

participating Tribes were surveyed concerning the federal entities, state entities, local entities, and other tribes with whom each participating Tribe has achieved some communications interoperability. Graph 18, below, depicts the number of border Tribes who have achieved some communications interoperability with other entities and/or tribes.

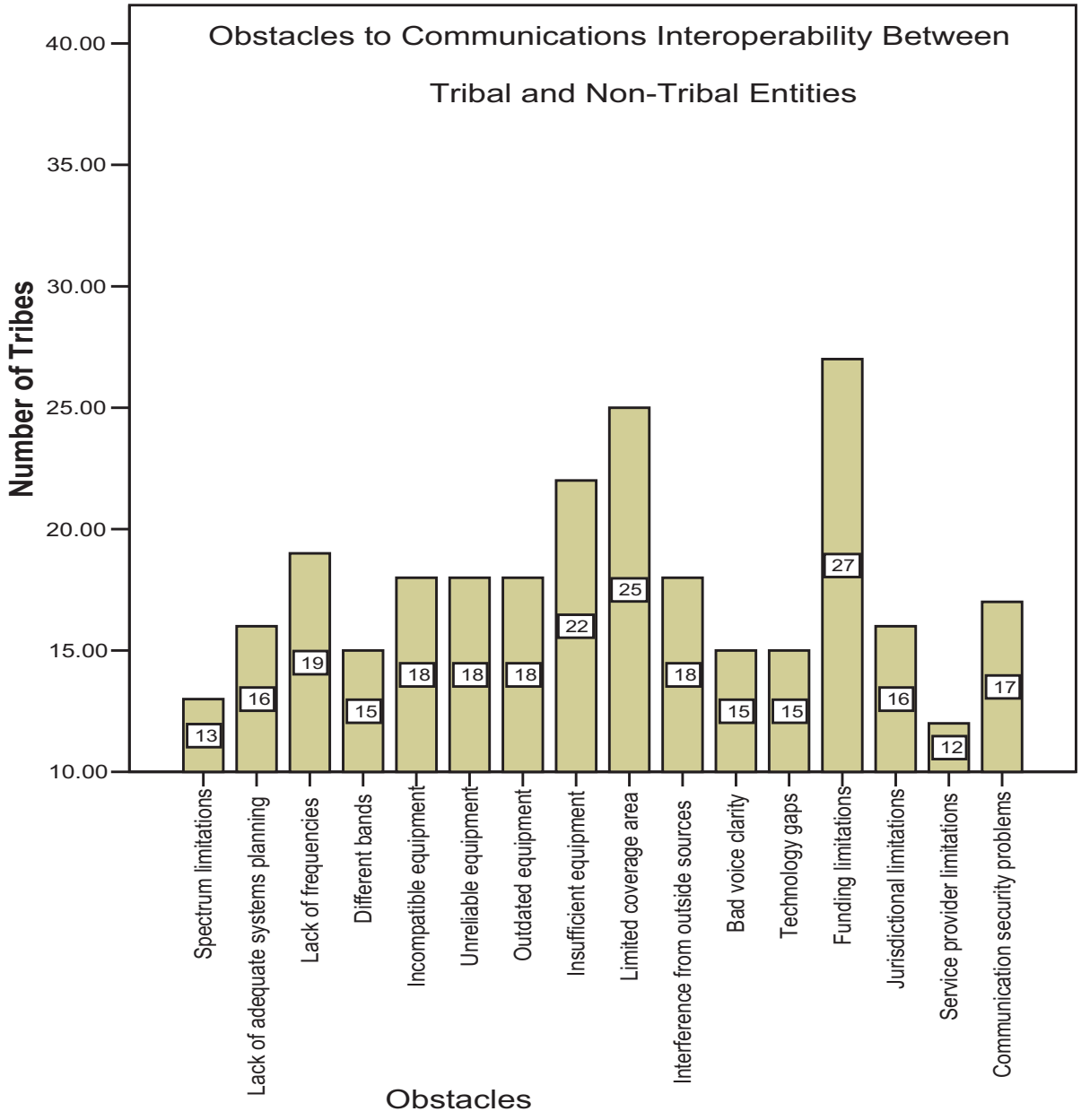
Graph 18



As revealed in Graph 18, the most prevalent communications interoperability achieved by border Tribes is between themselves and local entities.

With regard to the baseline for comparison of the border Tribes' obstacles to communications interoperability, the forty (40) participating Tribes were surveyed concerning certain types of obstacles to communications interoperability. The specific obstacles inquired about included: spectrum limitations, adequacy of systems planning, frequencies, bands, equipment compatibility, equipment reliability, equipment technology, equipment quantities, coverage areas, interference, voice clarity, technology gaps, funding limitations, jurisdictional limitations, service provider limitations, and communication security problems. Graph 19, page 41, depicts the number of border Tribes encountering each type of obstacle to communications interoperability.

Graph 19



As revealed in Graph 19, the most common obstacles to communications interoperability encountered by the border Tribes is funding limitations.

B. Tribal Border Security Interoperable Communications Best Practices.

The information shared by the participating Tribes in the TBS Pilot Program reveals a number of tribal border security best practices with regard to the Communications and Information Management function. One best practice is that several border Tribes have an established contact with U.S. Customs and Border Protection, U.S. Coast Guard, State police departments, and/or local police departments. A second best practice is that 72% of the participating border Tribes have at least some communications system compatibility

with the federal, state, or local emergency communications systems. Finally, a third best practice is that 80% of the participating border Tribes are capable of communicating with the Department of Homeland Security by computer.

C. Tribal Border Security Interoperable Communications Alerts.

The information shared by the participating Tribes in the TBS Pilot Program reveals a number of tribal border security alerts with regard to the Communications and Information Management function. One border security alert is that the median range of communication "dead spots" on Tribal lands is 21% to 30%. A second border security alert is that the median number of times per month that tribal emergency responders lose communication with their respective communications dispatch is 11 to 20 times per month. A third border security alert is that 28% of the participating border Tribes reported that their respective communications system, if any, is not compatible with any federal, state, or local emergency communications system. A fourth border security alert is that only around half of the participating border Tribes reported that they have achieved some communications interoperability with federal or state entities. Lastly, a fifth border security alert is that each of the communications interoperability obstacles identified in the survey were cited as obstacles by twelve (12) or more border Tribes, with the most common obstacle to communications interoperability being funding limitations.

Border Security In Terms Of The National Preparedness Goal: Critical Infrastructure

Critical infrastructure refers to the vital systems and assets of a community -- the incapacity or destruction of which would have a debilitating impact on that community and perhaps beyond. Protection of critical infrastructure vital to the United States is a target capability of the evolving Target Capabilities List, and is therefore relevant in assessing border security.[1] The desired outcome is that "[a]t-risk and vital targets are identified; vulnerability assessments are conducted, documented, and standardized, consequences are assessed, current mitigation capabilities are determined, and the threat to, and vulnerability of, high-risk targets are reduced."[2]

In the TBS Pilot Program, the forty (40) participating Tribes shared information pertaining to their respective critical infrastructure. The information shared, when analyzed in the aggregate, reveals a tribal border security baseline, as well as certain best practices, and alerts relevant to the critical infrastructure protection capability. The baseline and the best practices and alerts are each summarized in turn.

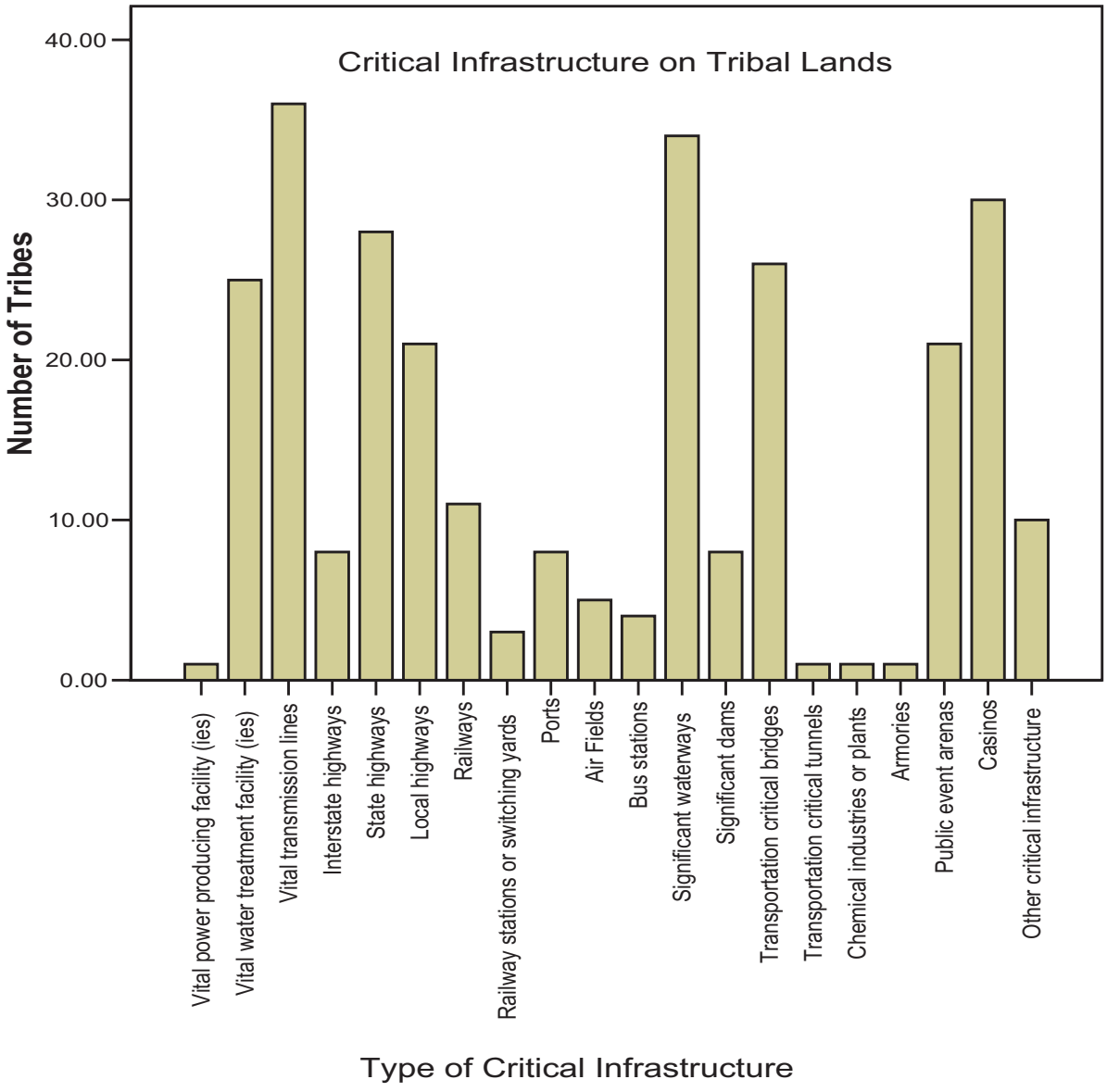
A. Tribal Border Security Critical Infrastructure Baseline.

The information shared by the participating Tribes in the TBS Pilot Program reveals a baseline for comparison of the critical infrastructure located on the lands of the participating border Tribes. More particularly, the forty (40) participating Tribes were surveyed concerning the types of critical infrastructure located on their respective lands. The specific types of critical infrastructure included in the survey were the following: vital power producing facilities, vital water treatment facilities, vital transmission

[1] *See Target Capabilities List: Version 1.1*, U.S. Department of Homeland Security, May 23, 2005, p. 49.
[2] *Id.*

lines, interstate highways, state highways, local highways, railways, railway stations or switching yards, ports, air fields, bus stations, significant waterways, significant dams, transportation critical bridges, transportation critical tunnels, chemical industries or plants, armories, public event arenas, and casinos, among others. Graph 20, below, depicts the number of borders Tribes who reported the presence of each type of critical infrastructure on their respective lands.

Graph 20



As revealed in Graph 20, the most prevalent type of critical infrastructure located on the lands of the border Tribes is vital transmission lines.

B. Tribal Border Security Critical Infrastructure Best Practices.

The information shared by the participating Tribes in the TBS Pilot Program reveals a number of tribal border security best practices with regard to the critical infrastructure protection capability. One best practice is that some Tribes have determined the vulnerabilities of the critical infrastructure located on their respective lands.[1] A second best practice is that some Tribes have determined the interdependencies of the critical infrastructure located on their respective lands.[2] Finally, a third best practice is that some Tribes have determined the protection incentives of the critical infrastructure located on their respective lands.[3]

C. Tribal Border Security Critical Infrastructure Alerts.

The information shared by the participating Tribes in the TBS Pilot Program reveals a number of tribal border security alerts with regard to the critical infrastructure protection capability. One border security alert is that at least one border Tribe has every type of critical infrastructure identified in the survey located on its tribal lands. A second border security alert is that the vulnerabilities for 88% of the critical infrastructure located on the lands of the border Tribes has not yet been determined.[4] A third border security alert is that the interdependencies for 82% of the critical infrastructure located on the lands of the border Tribes has not yet been determined.[5] A fourth border security alert is that the protection incentives for 83% of the critical infrastructure located on the lands of the border Tribes has not yet been determined.[6] As such, it can be surmised that, with only a few exceptions, the overall impact to the border Tribes and to the country as whole of the incapacity or destruction (i.e., from a terrorist attack or natural disaster) of the critical infrastructure systems and assets located on the lands of the border Tribes is not presently known.

[1] Vulnerabilities are the characteristics of an asset's design, location, or operation/use that render it susceptible to damage, destruction, or incapacitation by terrorist or other intentional acts, mechanical failures, and natural hazards. For cyber-specific assets, as well as the human and cyber elements of an asset, vulnerabilities may also be present as flaws in security procedures, software, internal system controls, or the design and use of an information or communication system that may affect the integrity, confidentiality, accountability, and/or availability of data or services. Vulnerabilities include flaws that may be deliberately exploited to affect that asset/system or to allow further access to other assets/systems, as well as those that may lead to failure due to inadvertent human actions or natural disasters.

[2] Interdependencies are two or more items, sectors, or so forth that are mutually dependent upon each other. Thus, if one fails, the other fails, which may then cause a number of other cascading effects.

[3] With regard to critical infrastructure and key resources, protection incentives are the motivating factors for implementing measures to protect the critical infrastructure and key resources (i.e., the number of interdependencies of a given critical infrastructure or key resource warranted the implementation of certain protection programs).

[4] *See* Footnote # 79, *supra*.

[5] *See* Footnote # 80, *supra*.

[6] *See* Footnote # 81, *supra*.

V. TRIBAL BORDER SECURITY BEST PRACTICES AND ALERTS IDENTIFIED DURING THE TBS PILOT PROGRAM SITE VISITS.

Two (2) site visits were conducted in the TBS Pilot Program. One site visit was with the Cocopah Tribe and the other site visit was with the Sault Ste Marie Tribe of Chippewa Indians. Each site visit is discussed in turn.

A. TBS Pilot Program Site Visit With The Cocopah Tribe.

One site visit in the TBS Pilot Program was performed with the Cocopah Tribe, who graciously agreed to participate in the site visit. The tribal lands of the Cocopah Tribe adjoin the U.S. border with Mexico, and also adjoin the Colorado River. Representatives from the Cocopah Tribe,[1] DHS, NNALEA, NCAI, the Office of Homeland Security for the State of Arizona, U.S. Customs and Border Protection, Federal Bureau of Investigations ("FBI"), Bureau of Alcohol Tobacco and Firearms ("ATF"), the Quechan Tribe of Fort Yuma, Yuma County Sheriff's Department, Somerton Fire Department, and East Central University, among many others, participated in this site visit.[2] During the site visit, the Cocopah Tribe provided briefings and site tours on border security topics such as: emergency management; critical infrastructure; communications interoperability; and border protection. In return, the Cocopah Tribe received briefings and training on topics such as: DHS's Homeland Security Information Network (HSIN); NIMS Certification Training and Testing;[3] the NRP; Partnership Opportunities (i.e., between federal, state, local, tribal, and private entities); FBI's Distance Learning, Internet Learning, and CJIS LEO Services; ATF's National Integrated Ballistic Information Network (NIBIN);[4] and the State Emergency Powers Act. From this site visit, a number of tribal border security best practices and alerts were revealed.

1. Border Security Best Practices of the Cocopah Tribe.

The Cocopah Tribe has several border security best practices. These best practices were shared by the Cocopah Tribe in response to the TBS Pilot Program Specific Survey, and were demonstrated during the site visit. Many of these best practices are highlighted in the following paragraphs.

One border security best practice is that the Cocopah Tribe has formed a homeland security committee for its Tribe. This committee is called the Tribal Emergency Response Committee ("TERC"). TERC was formed in 1998 by a tribal resolution. The members of TERC include but are not necessarily limited to the following: the Cocopah Police Department; the Cocopah Fire Department; the Cocopah Environmental Protection

[1] The Cocopah Tribe demonstrated a great showing at the site visit. Representatives of the Tribe who participated in the site visit included but are not limited to the following: the Chief of the Cocopah Tribe, Representatives of the Tribe's Tribal Council, the Chief and other Representatives of the Cocopah Police Department, the Chief of the Cocopah Tribe Fire Department, Representatives of the Cocopah Tribe's Public Works Department, Representatives of the Cocopah Tribe's Environmental Protection Department, Representatives of the Cocopah Tribe's Tribal Emergency Response Committee, Representatives of the Cocopah Casino, Representative of the Cocopah Tribe's Public Relations Department, Tribal Elders and Leaders of the Cocopah Tribe, and other Members of the Cocopah Tribe.

[2] Senator Ben "Nighthorse" Campbell was a site visit luncheon guest.

[3] The NIMS Certification Training and Testing was conducted by East Central University.

[4] National Integrated Ballistic Information Network (NIBIN) Program - As each fingerprint is different, a firearm leaves unique, identifiable characteristics on expelled ammunition. ATF's NIBIN Program employs the Integrated Ballistics Identification System to compare images of ballistic evidence (projectiles and cartridge casings) obtained from crime scenes and recovered firearms. As new images are entered, the system searches the existing data base for possible matches that must be confirmed by a firearms examiner.

Agency; the Tribal Council of the Cocopah Tribe; the Cocopah Public Works Department; the Cocopah Health Maintenance Department; and the Cocopah Planning Committee. The Resources of TERC include a mobile command vehicle, satellite internet, satellite telephone, an upgraded 2-way communications system, global positioning systems, night vision, and personal protective equipment. Some of the recent achievements of TERC are: (a) participation in a mock countywide exercise regarding the re-enactment of a flood scenario; (b) development of a tribal specific incident management plan;[1] (c) development of a bio-terrorism response plan; (d) development of a quick reference flip chart for use by tribal employees;[2] (e) participation in a three year homeland security exercise with the State of Arizona; (f) development of relationships with non-tribal entities; (g) identification and prioritization of response equipment needed by the Cocopah Tribe;[3] and (h) acquisition of certain response equipment within the funding capabilities of the Cocopah Tribe.

A second border security best practice is that the Cocopah Tribe engages in communications interoperability with certain state and local entities. For example, the Cocopah Police Department and the Cocopah Fire Department participate in communications interoperability with the Arizona Department of Homeland Security, the Arizona Department of Emergency Management, the Public Safety Communications Committee, the Southern Regional Homeland Security Advisory Council, the Yuma Regional Communications System, and other Yuma area public safety agencies. In addition, the Cocopah Tribe has a mutual aid agreement with Somerton, Arizona, and is included in the Yuma Auxiliary Communications System (which is a back-up communications system).

A third border security best practice is that the Cocopah Tribe has performed an assessment of one of its most vital critical infrastructures, namely its Cocopah Casino. This assessment included an assessment of the vulnerabilities, interdependencies, and protection incentives of said critical infrastructure.

A fourth best practice is that the Cocopah Tribe has implemented a number of measures to stop smuggling activities and to increase the protection of its borders. Those measures include but are not necessarily limited to the following: heightened border patrols; clear-cutting of tribal lands adjoining the Colorado River and of the tribal lands bordering Mexico; road and gateway closings; and road, path, and gateway blockades (i.e., rock blockades).[4]

[1] The Cocopah Tribe's Tribal Specific Incident Management Plan will serve as a comprehensive operating manual for incidents. More particularly, the Plan covers the following with regard to each incident set forth therein: potential sources of the incident; incident management leaders; initial response; notification process; incident management; and response follow-up.

[2] The Quick Reference Flip Chart lists a number of incidents that might be encountered by the Tribe, and sets forth the steps to be performed in responding to each of the incidents listed. The incidents covered in the Flip Chart include: civil disturbance, propane leak, power outage, flood/water line break, an act of terrorism, suicide threat, earthquake, evacuation, suspicious mail, hazardous material spill, fire, bomb threat, and medical emergency.

[3] The response equipment needed by the Cocopah Tribe include but is not limited to mobile generators, plotter for mapping infrastructure, and a stationary generator.

[4] The U.S. Customs and Border Protection, Yuma Station, also stated during the site visit that it too was employing measures to combat smuggling activities and to promote border protection, including: smart surveillance technologies, additional personnel, lighting, fences, and brush clearance.

2. Border Security Alerts Identified during the Cocopah Tribe Site Visit.

During the site visit with the Cocopah Tribe, the Tribe, as well as other non-tribal entities such as U.S. Customs and Border Protection, Yuma Station, identified a number of border security alerts. Many of these alerts are set forth in the following paragraphs.

One border security alert is that there is a great deal of smuggling activities being encountered by the Cocopah Tribe across its borders. The Cocopah Tribe advised that some illegal aliens are paying smuggling cartels $7,000.00 to be smuggled across the border, and that from January 2005 through September 2005 approximately 188 "drive-ins" (i.e., wherein vehicles full of illegal aliens are driven across the border from Mexico and onto the Cocopah Tribe's lands) have been encountered by the Tribe. The Cocopah Tribe advised that in addition to the smuggling of illegal aliens, they have encountered a great deal of drugs and firearms smuggling. The Cocopah Tribe advised that these smuggling activities are being pursued through activities such as: (a) trails and pathways that have been made and marked by smuggling cartels -- these trails and pathways are traversed by both foot and automobile; (b) illegal alien hideouts located in thick vegetation; (c) sandbag bridges erected across the Colorado River by smuggling cartels -- these bridges are traversed by both foot and/or automobile; and (d) armed escorts provided by smuggling cartels.[1]

A second border security alert pertains to the pressing obstacles to the achievement of border security that were identified during the site visit. These obstacles include the following: (a) an increase in violent confrontations between smuggling cartels and law enforcement in the wake of increased border security initiatives; (b) an invasion by non-law enforcement citizen/patriot patrol watch groups; (c) an increase in the commission of violent crimes (i.e., murders, assaults, robberies) committed on tribal lands by Mexican Nationals on illegal aliens crossing the border; (d) generation differences regarding border protection measures (i.e., a desire for preservation of a known way of life that is free from closed roads, clear cut land, etc.); (e) the need for additional border patrol officers; (f) geographic limitations;[2] (g) identity issues;[3] (h) jurisdictional limitations; and (i) funding limitations.

A third border security alert pertains to problems with communications interoperability funding. More particularly, problems have been encountered regarding the availability of grants and other funding for communications interoperability. In addition, the timing of communications system decisions has not always been compatible with the timing of grant availability. For instance, a tribe may commit to expend its communications funding on a particular system that is currently being used for communications interoperability, and subsequently, a new communications system is rolled-out (i.e., after the tribe has already expended its funding on the old system).

---

[1] The U.S. Customs and Border Protection, Yuma Station, advised that between January 2005 through September 2005, it encountered the following smuggling activities, among others, in its area of coverage: (a) 135,000 illegal alien apprehensions -- of these apprehensions, 1,600 were citizens of countries other than Mexico, including countries suspected of terrorism; (b) 37,000 lbs. of marijuana confiscated; and (c) 1,252 conveyance seizures.

[2] For instance, the Cocopah Tribe is comprised of three reservations, which are not contiguous. In addition, the Cocopah Tribe extends into Mexico.

[3] For instance, some tribal members do not have passports and do not have birth certificates, which makes border crossings at regulated sites more difficult. Such is even more frustrating for tribal members who freely (i.e., without the necessity of showing credentials) crossed the border prior to the sites being regulated.

B. TBS Pilot Program Site Visit With The Sault Ste. Marie Tribe of Chippewa Indians.

A second site visit in the TBS Pilot Program was performed with the Sault Ste. Marie Tribe of Chippewa Indians, who graciously agreed to participate in the site visit. The tribal lands of the Sault Ste. Marie Tribe of Chippewa Indians adjoins approximately 100 miles of waterway border that separates the United States from Canada. Representatives from the Sault Ste. Marie Tribe of Chippewa Indians,[1] NNALEA, U.S. Customs and Border Protection, U.S. Coast Guard, the Federal Bureau of Investigations ("FBI"), and the Chippewa County Sheriff's Department, among many others, participated in this site visit. During the site visit, the Sault Ste. Marie Tribe of Chippewa Indians provided briefings and site tours on border security topics such as: emergency management; critical infrastructure; communications interoperability; and border protection. In return the Sault Ste. Marie Tribe of Chippewa Indians received briefings from non-tribal entities on their views of border protection and future partnership opportunities. From this site visit, a number of tribal border security best practices and alerts were revealed.

1. Border Security Best Practices of the Sault Ste. Marie Tribe of Chippewa Indians.

The Sault Ste. Marie Tribe of Chippewa Indians has several border security best practices. These best practices were shared by the Sault Ste. Marie Tribe of Chippewa Indians in response to the TBS Pilot Program Specific Survey, and were demonstrated during the site visit. Many of these best practices are highlighted in the following paragraphs.

One border security best practice pertains to the Sault Ste. Marie Tribe of Chippewa Indians' participation in a Community Flu Clinic and Mass Prophylaxis Exercise in October 2005.[2] This Exercise utilized the Incident Command System and was a success. Participants in the Exercise, in addition to the Sault Ste. Marie Tribe of Chippewa Indians, included but were not limited to the following: the Bay Mill Indian Community; War Memorial Hospital; Lake Superior State University; Hiawatha Behavioral Health; American Red Cross; U.S. Coast Guard, the Chippewa County Health Department; and the Chippewa County Office of Emergency Services.

A second border security best practice pertains to the Sault Ste. Marie Tribe of Chippewa Indians' cooperative agreements and patrols with non-tribal entities. For example, the Tribe has a cooperative agreement with the Chippewa County Sheriff's Department regarding the use of its canine unit for human and narcotic tracking. In addition, the Tribe has cross-deputized officers with the County. Another example, is that the Tribe has performed a number of joint border patrols with federal entities.

[1] The Sault Ste. Marie Tribe demonstrated a great showing at the site visit. Representatives of the Tribe who participated in the site visit included but were not limited to: the Chief of Police of the Sault Ste. Marie Tribe of Chippewa Indians, Representatives of the Sault Ste. Marie Tribal Police Department, Representatives of the Tribe's Casinos, Representatives from the Tribe's Judicial Branch, Representatives from the Tribe's Administrative Offices, Representatives from the Tribe's State-of-the-Art Juvenile Detention Facility, and other Members of the Tribe.

[2] This Exercise was performed during the site visit, so the TBS Pilot Program Site Team Members were able to observe this Exercise firsthand.

A third border security best practice pertains to the Sault Ste. Marie Tribe of Chippewa Indians' participation in community watches and outreach programs targeted at border security. An example of such a watch is the U.S. Customs and Border Protection's "Operation Riverwatch."

A fourth border security best practice pertains to the Sault Ste. Marie Tribe of Chippewa Indians' attendance at meetings of the Integrated Border Enforcement Team ("IBET"). IBET is an intelligence group pertaining to border security. IBET Members include but are not necessarily limited to: U.S. Customs and Border Protection; U.S. Coast Guard; Royal Canadian Mounted Police; Ontario Provincial Police, and the Canadian Border Services Administration.

2. Border Security Alerts Identified during the Sault Ste. Marie Tribe of Chippewa Indians Site Visit.

During the site visit with the Sault Ste. Marie Tribe of Chippewa Indians, the Tribe, as well as other non-tribal entities such as U.S. Customs and Border Protection, Sault Ste. Marie Station, identified a number of border security alerts. Many of these alerts are set forth in the following paragraphs.

One border security alert is that the Sault Ste. Marie Tribe of Chippewa Indians, as well as other non-tribal entities (i.e., U.S. Customs and Border Protection; U.S. Coast Guard) must safeguard a seasonal border. That is, in the summer the Tribe's border is water, while in the winter the Tribe's border is ice. Accordingly, the Tribe and non-tribal entities patrolling the border must not only possess water patrol capabilities (i.e., boats), but must also possess snow patrol capabilities (i.e., snowmobiles).

A second border security alert pertains to the pressing obstacles to the achievement of border security that were identified during the site visit. These obstacles include but are not limited to the following: (a) manpower limitations;[1] (b) jurisdictional issues; (c) geographic limitations;[2] and (d) funding limitations. Fortunately, certain obstacles that have been recently encountered on the U.S. Border with Mexico (such as an increase in violent confrontations between smuggling cartels and law enforcement, and an invasion of non-law enforcement citizen/patriot patrol groups) have not yet been encountered in the Sault Ste. Marie region.

Finally, a third border security alert is a concern expressed by site visit participants that as border security crackdowns are made with regard to the U.S. border with Mexico, smuggling cartels may turn their focus to the U.S. border with Canada. It was noted that the U.S. border with Canada is nearly twice as long as the U.S. border with Mexico, and therefore, it may soon become a greater target for smuggling cartels, criminals, and potential terrorists.

[1] At the time of the site visit, the U.S. Customs and Border Protection, Sault Ste. Marie Station, had approximately twenty-four (24) agents for a coverage area that encompasses thirty (30) counties, twenty-four thousand (24,000) square miles of land, a four hundred thousand (400,000) person population base, and four hundred and twenty (420) miles of lakeshore and riverbank border.

[2] For instance, the tribal lands of the Sault Ste. Marie Tribe are not contiguous.

VI. CONCLUDING REMARKS.

The TBS Pilot Program was a huge success, and could not have been accomplished without the willing participation of the numerous Tribes, their tribal leaders and communities, as well as the support of the Department of Homeland Security and the numerous Federal, State, Local, and Private entity advisors and participants. As President Bush recently stated: "America is grateful to those who are on the front lines of enforcing the border."[1]

With the TBS Pilot Program now complete, America has successfully taken another major step in its comprehensive assessment of its border and homeland security preparedness. America must continue to see this assessment through to completion. In the TBS Pilot Program twenty (20) baselines for comparison, thirty-eight (38) best practices, and forty-seven (47) alerts on the issues of border security generally and border security in relation to the National Preparedness Goal were identified. By participating in the TBS Pilot Program, the participating border Tribes have again demonstrated their desire to protect their respective communities as well as America as a whole.

Subsequent programs lawfully patterned after the TBS Pilot Program would render a complete set of baselines, best practices, and alerts that could be used to effectively, fairly, and consistently assess preparedness and future border and homeland security investment justification initiatives. Without the performance of these additional programs, the national and uniformed preparedness standard sought, will remain elusive, thereby hampering decision makers ability to determine the most beneficial future investment justification initiatives. It is doubtful that border and homeland security can ever be achieved at its most optimal level without this national and uniformed standard.

[1] *See President Discusses Border Security and Immigration Reform in Arizona*, Tucson, Arizona, Davis-Monthan Air Force Base, November 28, 2005.