Impacts of Federal Cyber Security Mandates on the Private Sector

Robert Oddo
GIAC Security Essentials Certification (GSEC)
Raleigh, NC (May 2003)
Practical Assignment Version 1.4b, Option 1

TABLE OF CONTENTS

1 Abstract

The internet is increasingly under attack from a host of malicious sources. The potential risk for debilitating cyber attacks against public and private sector organizations is increasing every day and there is growing concern on the ability of our critical information infrastructure to withstand such an attack. The Federal Government is taking a leading role in the development of cyber security mandates and initiatives. These come in many forms including federal law, industry directives, best practices and procurement policies. In this report, we will explore, in some detail, the meaning of the most significant legislation and directions that government has provided in the cyber security area. These touch all facets of public and private institutions and will have a profound impact on not only the way business is conducted but also the technological innovation that will be required to satisfy these initiatives.

This document will review three major federal mandates, Homeland Security, the Patriot Act of 2001 and the National Strategy to Secure Cyberspace and their potential impact on the private sector information technology and their security requirements.

Information technology and security professionals will be challenged to meet a sometimes bewildering array of requirements that will need to be implemented in a short period of time, and at the expense of current budgets and existing projects. This report will attempt to highlight the key areas in which greater involvement either is already on going or is anticipated, as well as highlighting key requirements and their associated impacts. The report will conclude with some key recommendations for information technology security personnel. This will help prepare them for the government mandates and initiatives that will help to ultimately reduce overall security vulnerabilities and increase their organizations ability to withstand and respond to them before, during and after the threat occurs.

2 Introduction to Federal Mandates

Since the beginning of 2001, the federal government recognized the importance of addressing cyber security through legislation. The most significant of all these mandates that will be covered here are the Department of Homeland Security, The US Patriot Act of 2001 and the National Strategy to Secure Cyber space.

2.1 Homeland Defense

The first mandate is the formation of the Department of Homeland Security[1] (DHS). This was created through the passage of the Homeland Security Act of 2002. This came out of the realization that the country was ill prepared for the kind of terrorist attack like the one that occurred on 9/11. This ambitious plan by the government will take 22 different government organizations and unify them under a single government agency that will improve protection against today's and tomorrow's threats. The three primary missions include:

- Prevent terrorist attacks within the United States
- Reduce America's vulnerability to terrorism
- Minimize the damage from potential attacks and natural disasters

Agencies falling under DHS include Department of Transportation, Department of Justice, Coast Guard, U.S. Customs and many security-related departments of other agencies (for instance, the Nuclear Incident Response Team will move from the Department of Energy to DHS).

The DHS continues to evolve its' organization and has established four major directorates: Border and transportation Security, Emergency Preparedness and Response, Science and Technology, and Information Analysis and Infrastructure Protection, all under the direction of Secretary Tom Ridge.

Included in the DHS mandates were provisions that address the protection of cyberspace that are listed below. The impact of these will be addressed in the next section in more depth. The most important of these mandates include:

1. Requiring federal agencies meet a baseline level of computer security that is technology and product neutral. Included in the act was the Federal Information Security Management Act of 2002. This provides a broad mandate on the DHS to oversee all Federal Information Security. Included in this is the creation of a framework for ensuring effectiveness of all information security that supports Federal operations; government oversight and management of all information security risks including coordinating with civilian agencies; developing the necessary controls to protect Federal information and information systems as well as allowing agencies to use commercial security products to fulfill these tasks.
2. Maintaining the separation of NIST's (National Institute of Standards and Technology, part of the US Department of Commerce) Computer Security Division from the Department of Homeland Security. NIST is responsible for developing the information security standards that will be implemented in the first mandate listed above in number 1.
3. Creating an Undersecretary for Information Analysis and Infrastructure. This position was filled by Frank Lubutti and confirmed by unanimous vote of the Senate in June 2003. This is one of the four Directorates under Secretary Ridge that will help solve the information flow roadblocks that helped contribute to 9/11. This is the key organization that will effect both public and private IT organizations.
    - Specifically this directorate is mandated to integrate information from law enforcement, intelligence organizations and other sources to detect and assess terrorist threats; carry out comprehensive vulnerability assessments of key resources and critical infrastructure; integrate information in order to identify protective and support priorities; administer

homeland security advisory system; establish a secure communications and information technology infrastructure; and, in general, review, analyze and make recommendations on the collections, dissemination, sharing and standards of any security-related information.

4. Provide liability protection for information technology companies who develop anti-terrorism technologies, goods and services. Through the SAFETY Act, or the Fostering Effective Technologies Act of 2002, once an anti-terrorism technology has been approved by the Secretary of Homeland Defense the government will extend to these vendors special treatment rules and a federal jurisdiction for claims arising from the use of their products.

5. Establishing a mechanism to help the local communities respond and recover from attacks on information systems and communications networks. Through an expansion of the role of the Federal Emergency Management Agency (FEMA), there are specific measures put into place to help rebuild these facilities as well as measures for protecting and restoring critical infrastructure and assets that have been damaged by attack.

6. Promoting the voluntary sharing of information about cyber security threats and solutions. In section 221, specific procedures have been outlined to share information between public and private sector organizations. Threat warning systems will continue to be enhanced and best security practices will be fostered through this organization.

7. Increasing penalties for computer-related crimes through the Cyber Security Enhancement Act. This established specific modifications of the US Criminal Code that provided specific penalties for computer crimes. Included in this is classification of computer crimes as felonies, mandatory sentences and a federal jurisdiction for prosecuting these crimes.

2.1.1 Impact of Homeland Security Mandates

To look at the complexity of the overall mandates, let us use the proposed Border Security process[2] as a typical example. In the process of issuing visas, controlling entry, managing stays and controlling exit there are no less then 10 major government organizations all at different levels.

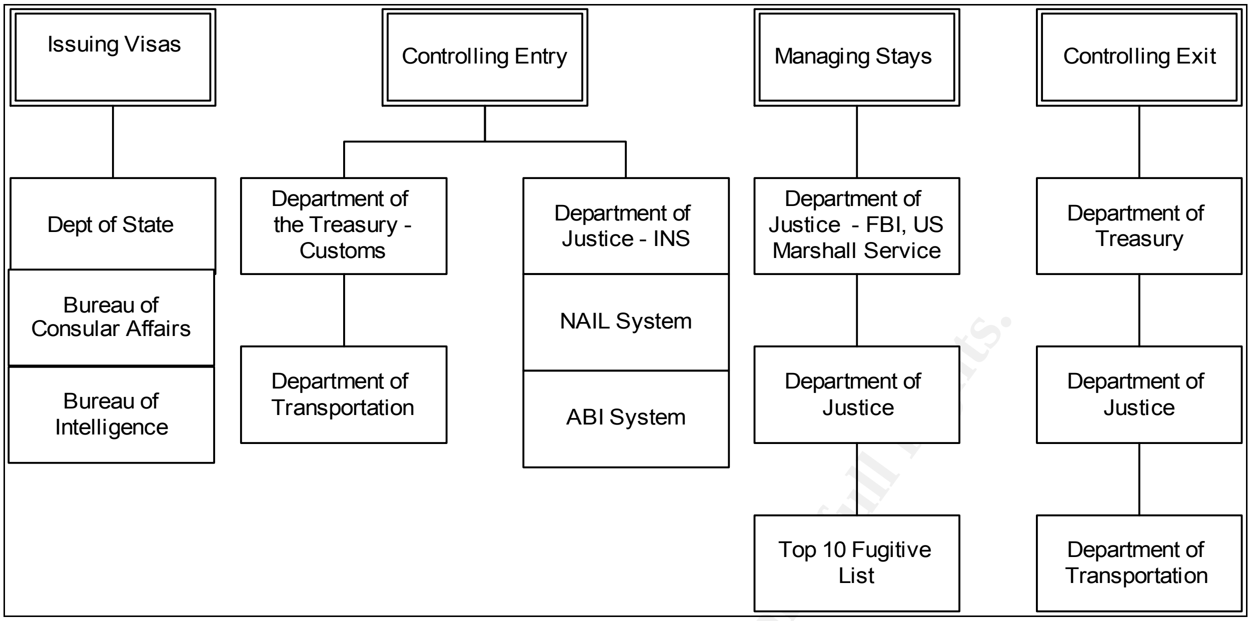


Figure 1 Border Security Process (Simplified) [3]

While the above diagram does not fully illustrate the complexity of the information technology support that needs to be in place to support this infrastructure, it is highly dependant on a tightly coupled information flow. This is an excellent example of the complexity of the various inter-agencies, and well as private sector, information that must be integrated into a cohesive system. The impediments to integration are vast considering the 10 agencies all have different legacy information technologies, architectures, data schemas and so forth in place supporting their current mission. Setting requirements, standards and establishing funding to promote the necessary changes will be up to the Information Analysis and Infrastructure Directorate.

To support the security implications of such large-scale integration, a number of critical practices have come forward from NIST (National Institute of Standards and Technology - http://www.nist.gov/) specifically to address the security awareness generated by the Homeland Defense mandates. These are highlighted on their website as Federal Agency Security Practices (FASP) (http://csrc.nist.gov/fasp/).

> *"The FASP effort was initiated as a result of the success of the Federal CIO Council's Federal Best Security Practices (BSP) pilot effort to identify, evaluate, and disseminate best practices for CIP and security. NIST's Computer Security Division was asked to undertake the transition of this pilot effort to an operational program. As a result, NIST developed this web site. The FASP site contains agency policies, procedures and practices; the CIO pilot BSPs; and, a Frequently-Asked-Questions (FAQ) section. The FASP site differs from the BSP pilot in material provided and in complexity."* [4]

While primarily directed at Federal Security professions, these have broad applicability to the private sector as well. Key areas that are covered include:

- Audit Trails
- Certification and Accreditation Processing
- Contingency Planning
- Data Integrity
- Documentation descriptions
- Hardware and System Software Maintenance
- Identification and Authentication
- Incident Response Capability
- Life Cycle
- Logical Access Controls
- Network Security
- Personnel Security
- Physical and Environmental Protection
- Production, Input/output Control
- Policy and Procedures
- Program Management
- Review of Security Controls
- Risk management
- Security Awareness
- System Security plan

Complete descriptions of these, as well as the best practice documents, can be found at http://csrc.nist.gov/fasp/index.html . The importance of a resource such as this, as well as others found at http://csrc.nist.gov/fasp/index.html will be clear in the next section as we examine the impact the government mandates.

NIST also has published Special Publication 800-37, *Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems*, in order to establish a standard process to certify and accredit IT systems supporting the executive branch of the federal government. While this process focuses on federal systems processing, storing and transmitting sensitive (unclassified) information, the associated tasks and subtasks have been broadly defined to be universally applicable to all types of IT systems.

These two efforts should be widely noted by the private sector as they have direct applicability as either a best practice or as a requirement to do business with the government.

2.2 Patriot Act

Second in the series of cyber security mandates is the USA Patriot Act of 2001, which provides laws to deter and punish terrorist acts in the US and around the world, enhance law enforcement investigatory tools as well as provide specific additional mandates. This act makes changes to over 15 different statutes. There are many provisions in this act, but the major ones that impact the private sector include Title I: Enhancing Domestic Security Against Terrorism; Title II: Enhanced Surveillance Procedures and Title III and International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001.[5] Specific mandates include:

- Title I
  - Requires the Director of the Secret Service to develop a network of electronic crime task forces to prevent, detect and investigate various

forms of electronic crimes including potential terrorist attacks against critical infrastructure and financial payment systems.

- Title II:
    - Enhances surveillance Procedures by amending the Federal criminal code to authorize the interception of wire, oral and electronic communications for the production of evidence of terrorism offenses and computer fraud and abuse.
    - Permits the seizure of voice-mail messages under a warrant
    - Expands the scope of subpoenas for records of electronic communications to include the length and types of service utilized, temporarily assigned network addresses, and the means and source of payments (including any credit card or bank account number).
- Title III:
    - Amends Federal law governing monetary transactions to prescribe procedural guidelines under which the Treasury may require domestic financial institutions to take specified measures.
    - Creates regulations requiring registered securities brokers to file reports of suspicious financial transactions

2.2.1 Impact of the Patriot Act

Unlike the partnership approach of Homeland Security, the USA Patriot Act of 2001 takes a more statutory approach that already has the private sector closely examining the overall impact.

While there is much controversy on the impact of civil liberties stemming from this Act, key requirements have already affected financial institutions. New requirements for transaction reporting were mandated, and quickly implemented, by these institutions.

In the above case, the Treasury ruled that Section 326 of the Act requires that financial institutions develop a Customer Identification Program (CIP) that implements reasonable procedures to:

1) Collect identifying information about customers opening an account
2) Verify that the customers are who they say they are
3) Maintain records of the information used to verify their identity
4) Determine whether the customer appears on any list of suspected terrorists or terrorist organizations

Organizations effected by just this ***one*** section noted above, were:

- Banks and trust companies
- Savings associations

- Credit unions
- Securities brokers and dealers
- Mutual funds
- Futures commission merchants and futures introducing brokers

ALL which needed to enhance their current systems to adhere to these new requirements.

Likewise, the act requires *real-time* interception of non-content information including dialing, routing, addressing, signaling information, IP addresses and port numbers, to and from information in e-mail headers. This is in addition to the already established ability to wiretap real-time interception of electronic communications under Section 18 of the US Code.

2.3 National Strategy to Secure Cyberspace

Third in the series of cyber security mandates is The National Strategy to Secure Cyberspace[6]. The final version of which was released by the government on February 14, 2003. While technically not a mandate in approach, the strategy lays out specific issues and initiatives for all its' effected constituency, which includes federal agencies, state and local governments, private industries, educational institutions and citizens, following this key principle directive:

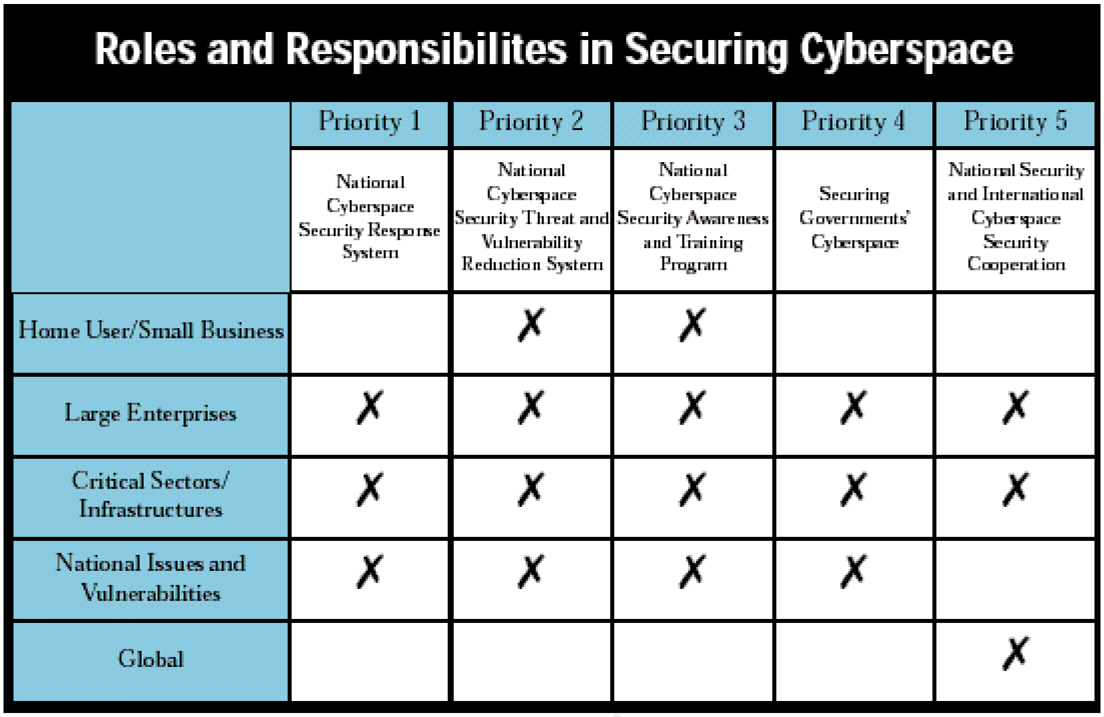
> *"…engage and empower Americans to secure the portions of cyberspace that they own, operate, control, or with which they interact. Securing cyberspace is a difficult strategic challenge that requires coordinated and focused effort from our entire society, the federal government, state and local governments, the private sector, and the American people."*[7]

A copy can be reviewed at http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf . (An interesting side note for the geeks among us. The title page includes a message in binary. Decoded, this is an invitation to comment on the document contents but, overall, is a very imaginary inclusion typically not seen in a government document!).

The strategy provides a framework to:[8]

- Prevent cyber attacks against critical infrastructures
- Reduce national vulnerability to cyber attacks
- Minimize damage and recovery time from cyber attacks that do occur.

Perhaps the most unique approach in this strategy, as can be seen in the following table, is the large degree empowerment and partnership required to implement the initiatives rather then regulation, which is the normal government approach. Much of the document orientation goes into detail on how to foster the public-private cooperation needed to implement the directives.



Roles and Responsibilites in Securing Cyberspace

	Priority 1	Priority 2	Priority 3	Priority 4	Priority 5
	National Cyberspace Security Response System	National Cyberspace Security Threat and Vulnerability Reduction System	National Cyberspace Security Awareness and Training Program	Securing Governments' Cyberspace	National Security and International Cyberspace Security Cooperation
Home User/Small Business		✗	✗		
Large Enterprises	✗	✗	✗	✗	✗
Critical Sectors/ Infrastructures	✗	✗	✗	✗	✗
National Issues and Vulnerabilities	✗	✗	✗	✗	
Global					✗

Table 1 - Roles and Responsibilities [9]

The chart above shows the critical priorities for cyberspace security as outlined by the strategy. Five national priorities are listed as well as "levels" at which action needs to occur on. The priorities are focused on improving the response to incidents, reduce the possibility of attack, and diminish our vulnerabilities as well as preventing attacks that could affect our national security. There are 31 total initiatives, of which the first three priorities directly call for private sector security initiatives. The most important of these include:

- The development of architectures that will allow for the identification, alerting and mitigation of any malicious activity. This is a complex partnership in which the government and private sector must not only coordinate efforts but also have their information systems hardened to operate under attack.

- Be able to reduce threats and vulnerabilities through improvements in our network infrastructure to withstand and mitigate any attacks as well as improving software to eliminate vulnerabilities that can be exploited.

- Increase the awareness of vulnerabilities through education and certification. Organizations must be advocates for stronger training and certification programs to increase staff skill levels necessary to understand, react and overcome any threat presented to their organization.

The way to create these public-private partnerships so critical to the implementation and success of the strategy has been through facilitation by the Partnership for Critical infrastructure Security (http://www.pcis.org/). As defined in the strategy, the following have been defined as critical infrastructure sectors:

- Banking and Finance
- Insurance
- Chemical
- Oil and Gas
- Electric
- Law Enforcement Higher Education
- Rail Transportation
- Information Technology and Telecommunications
- Water

Each of the above sectors is responsible for developing their own plan to address the security needs of that sector to reduce or eliminate threats and vulnerabilities.

It is clear that the government recognizes that the internet is vital to the US economy and intends on addressing the security concerns through a broad array of initiatives in a creative and compelling manner. Securing cyberspace is *everyone's* concern and that we all must work together is the strategic goal that must be accomplished and the strategy put the responsibility on both the Federal and private sectors to fulfill the initiatives.

2.3.1 Impact of the Cyber Security Strategy

Key to many of the government initiatives contained in this strategy is the amount of information sharing that must take place to enable the level of cooperation needed. Private industry, via the Partnership for Critical infrastructure Security (http://www.pcis.org/) mentioned earlier will have a forum to address these issues. However, the burden to make the necessary system and application changes necessary will be borne directly or indirectly (via fee recovery in some cases) by the private sector.

Fundamental issues that need to be resolved, include:[10]

- Establishing the necessary trust relationships between federal and non-federal entities. There has typically been a level of distrust between these entities that must be overcome through open communication and the establishment of strong partnerships.
- Developing Standards and Agreements on how shared information will be used and protected. Of great concern are civil liberties and the protection of vital information. There is a fine line between safeguarding rights and providing for a secure environment. This will be a constant struggle as forces seek to reduce civil liberties in the name of security. Organization will need to be empowered to seek the best balance between the two.

- Establishing effective and appropriately secure communications mechanisms. Necessary in the environment will be the establishment of trusted relationships and supporting credentials. Implicit in this is creating a chain of security within all organizations and processes, including the use of strong passwords, smart tokens and biometrics.

- Taking steps to ensure that sensitive information is inappropriately disseminated. Specific mechanisms are being put into place to prevent shared confidential information being release through the establishment of uniform procedures for how critical infrastructure information is classified and treated.

The National Strategy to Secure Cyberspace takes great pains to foster a strong public-private relationship to build the necessary collaboration to align and facilitate enhancements to critical IT infrastructures. For many of the industry sectors, however, this has been historically difficult to do. This is understandable considering the competitive issues as well as the issues listed above.

3 Conclusions

Homeland Security, the National Strategy to Secure Cyberspace, the USA Patriot Act of 2001 all share a common theme – they all affect the private sector information technology security organizations. Key challenges that will have to be overcome by IT organizations will be to effectively enhance their defense against cyber attacks, facilitate the exchange of information that allows the prevention or provides mitigation of such an attack, as well as meeting legal requirements to furnish information to the government. These will be felt by virtually every organization, public or private, right down to the individual citizen. At each level, new requirements have been mandated or are in various stages of being specified by government agencies or industry-working groups will have to be understood, absorbed, financed and implemented.

Key mandates, and their associated expense, will be borne by government agencies, private sector organizations, and ultimately the public who will pay for these enhancements in securing our nations cyber infrastructure. Those that will need to be accommodated in the private sector include:

- Developing blueprints for operational and technological change that facilitate secure information exchange. On the most basic level, this is one of the biggest challenges the federal sector must overcome as they integrate the disparate connectivity and interoperability issues at the database level. One another level, there is on-going architectural discussion already underway at the sector level through the ISACs (information Sharing and Analysis Centers) that have started to formalize information exchange among their members and take stock of the operational risks from cyber attack. IT professionals from these groups should already be working or be aware with what the ISACs are mandating. Refer to their web site at http://www.pcis.org/ for more detailed information or contacts.

- Increasing the ability, through the development of an active security policy in cooperation with the public-private sectors, to prevent, detect and identify threats, vulnerabilities and attacks. This will need to happen at both the software and network levels. At the basic level, the CERT Coordination Center has been providing vulnerability and attack information for some time. However, new security initiatives that take a more holistic approach are being put into place. As part of the critical infrastructure protection program, the IAIP (Infrastructure Analysis, Information Assurance directorate of the Department of Homeland Security has recently merged with the NIPC (National Infrastructure Protection Center), FedCIRC (Federal Computer Incident Response Center) and 3 other government entities. While this agency works diligently up front to collect and analyze threat information it will be up to the private sector organizations to have the tools, processes and infrastructure in place to react and mitigate any threat. This may involve implementing new technologies in private networks, upgrading or replacing software to fix vulnerabilities, increasing staff to be able to create and support necessary security policies and procedures as well as implementing separate control networks to minimize disruptions during DoS attacks.

- Meet legal requirements to provide electronic records and information at a level that is unprecedented. The government is demanding access to a greater amount of information, both paper and electronic, than ever before. Right now, there are few, if any, information exchange standards that can securely access and transfer this information. Without some preparation, tools and process in place many IT security organizations will be hard pressed to supply the requested information without an undue burden.

    - A case in point is that the Foreign Intelligence Surveillance Act of 1978 (FISA) authorized collection of business records in very limited circumstances, and mostly those relating to common carrier, vehicles or travel, and only via court order. The USA Patriot Act expands this collection to all “tangible things” including business records that may be obtained via a subpoena.

    - A more detailed look at the overall IT impact of just the search and seizure provisions of electronic information includes the following significant changes[11]: Basic subscriber information is now expanded to include payment information, session times and direction, as well as network addresses that must be provided.

    - Real-time interception of non-content information including dialing, routing, addressing, signaling information, IP addresses and port numbers to and from, as well as the information in e-mail header must be provided.

    - There are, in addition to the previous types of information sought, transaction records, e-mail in storage, e-mail that has been opened by the user, stored voice mails that were transmitted by computer and real-time interception of the content of electronic communications that must be accommodated. Typically, this request will come in the form of a subpoena.

Private sector IT organizations are already seeing the initial wave of mandates and the ensuing requirements that need to be met. These demands will only increase as organizations attempt to secure their own business assets while at the same time trying to understand, and meet, the necessary mandates being brought forward by the public sector. Organizations, small and large, must be prepared to meet the increasing demand that is being thrust upon them. Everything from software vulnerabilities, risk analysis, network upgrades and enhancements to provide better alerting, or collection of legal information based on a court order must be accommodated in the name of security.

Organizations should carefully note key initiatives that are being implemented and highlighted in this report, and assess the impacts on their organization. One place to start is by reviewing the best practices noted previously in this paper and noted in the reference section under the NIST FASP website. A review of these guidelines would be an excellent start to understanding what current security gaps exists and what securing the organization will take by addressing the identified gaps. Adoption and implementation of the NIST guidelines would provide a more secure foundation for any organization. Organizations are also encourage to review the IT security certification and accreditation guidelines as outlined in NIST 800-37 described earlier would help show that the minimum security control exist and are in place to secure the IT system.

Implementation of these best practices will lay the foundation for a strong security IT infrastructure that will more easily accommodate the demands of the government mandates and initiatives covered in this report.

4 References

[1] **The National Strategy For Homeland Security: Office of Homeland Security** http://www.whitehouse.gov/homeland/book/index.html

[2] GAO Testimony before the Committee on Government reform, House of Representatives. Homeland Security: Information Sharing responsibilities, Challenges, and Key Issues. May 8, 2003. http://www.iwar.org.uk/homesec/resources/gao/d03715t.pdf

[3] ibid, page 33

[4] NIST FASP website http://csrc.nist.gov/fasp/index.html

[5] **H.R. 3162 USA Patriot Act of 2001.** http://www.epic.org/privacy/terrorism/hr3162.html

[6] **The National Strategy to Secure Cyberspace** http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf

[7] From the web page at http://www.whitehouse.gov/pcipb/

[8] **The National Strategy to Secure Cyberspace,** page viii, http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf

[9] **The National Strategy to Secure Cyberspace,** page 9, http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf

[10] ibid, page 36

[11] American Library Association, Matrix, http://www.ala.org/Content/NavigationMenu/Our_Association/Offices/ALA_Washington/Issues2/Civil_Liberties,_Intellectual_Freedom,_Privacy/The_USA_Patriot_Act_and_Libraries/matrix.pdf