# Global Information Assurance Certification Paper

# CYBER-SECURITY AND INFORMATION SHARING ISSUES, CHALLENGES, AND ENABLING TECHNOLOGIES IN THE POST 9-11 GOVERNMENT.



David C. Wylie
GSEC Practical Version 1.4
June 16, 2002

**Table of Contents**

**Abstract**

The purpose of this paper is to provide an overview of the challenges that face the U.S. Government in the aftermath of the 9-11 attacks on the United States with a particular focus on cyber-security and information sharing challenges.

Enabling technologies which can facilitate cyber-security and information exchange are also described. Some of these technologies are currently available, while others are still in the development process. Finally, a short section postulating, in broad strokes, a "holy grail" of information sharing that would provide agency collaboration is outlined.

**Overview**

There are many agencies, offices, and services that play a part in the war on terrorism (and other crime) and their success in effectively waging that war is dependent largely on their ability to effectively share intelligence and do so securely and in a timely manner. The current roster of participants in this effort includes but is not limited to:

- Federal Bureau of Investigation (FBI)
- Central Intelligence Agency (CIA)
- National Security Agency (NSA)
- Department of Justice - Immigration and Naturalization Service (INS)
- Department of Justice - United States Border Patrol
- Department of Defense (DOD) - Defense Intelligence Agency (DIA)
- United States Coast Guard (USCG)
- Department of State (DOS)
- Department of Treasury - United States Treasury Service (USTS)
- Department of Treasury - United States Customs Service
- Department of Energy (DOE)
- Army Intelligence
- Navy Intelligence
- Air Force Intelligence
- Marine Corps Intelligence
- National Imagery and Mapping Agency
- National Reconnaissance Office
- State law enforcement agencies (50)
- Local and County law enforcement agencies (thousands)

This list, while nowhere near complete, serves its purpose by illustrating the vast number of civilian and military organizations that are involved in keeping our country safe from its enemies. By broadening our view to an international one, the challenge of communicating intelligence data with our coalition partners makes the problem an order of magnitude more complex.

## The Problem

In order for the United States to be effective in protecting its people, territory, and strategic interests, it must solve the problem of collecting, protecting, analyzing, and making information available to those who need it. The opposing needs for data protection and availability for use are challenges that must be met in order to succeed. Congress has recognized this need and passed a number of funding initiatives to address the problem, including the Cyber Security R&D Act of February 2002, allocating $1 Billion for research and education programs. [1]

The intelligence gathering, collation, and analysis at virtually all of the intelligence and law enforcement agencies in America takes place in a “stovepipe” environment. That is to say, pieces of information collected by agents of any given Federal agency are kept within the agency database. The data is rarely, if ever, shared with sister agencies, and with their more distant state, county, and local law enforcement cousins under even more exceptional cases.

The FBI, the lead US agency for dealing with domestic terrorism, is unable to perform its function because of antiquated technology. According to FBI Director Robert Mueller, the Bureau is "far behind current technology" and "cannot support the robust analytical capacity we need." [2]

Congressman Curt Weldon of Pennsylvania stated, “The 33 intelligence agencies have failed U.S. citizens by largely refusing to share information that would enable them to better picture what enemies are doing." [3] As an example of the inability of various agencies to share and communicate with one another, Weldon cited a case in 1997 when he and other lawmakers were traveling to Europe to assist in negotiations to end the war in Kosovo. The CIA was only able to provide him with two lines of information about the people with whom he was meeting. However, when Weldon contacted a Military Intelligence unit at Ft. Belvoir, VA they were able to provide him an eight-page profile. [5]

There are many obstacles that prevent effective communication and data sharing. Some of the most obvious are that these agencies have no common systems that allow them to share data, have very little desire to do so, and, in the case of state and local law enforcement, no capability to access sensitive material.

## Challenges

In order to share data between intelligence agencies and law enforcement offices a level playing field must be created. One of the greatest challenges is in unraveling the complex system by which the U.S. Government assigns levels of sensitivity to important documents and information. There are a number of systems and permutations of systems in use across the government.

***Military Classifications***
The U.S. Military classifies information on a hierarchical scale beginning with Unclassified and running up through Top Secret. Known collectively as the Collateral National Security Information, the classifications are:

- **Unclassified** (With six separate sub-classifications)
- **Confidential**
- **Secret**
- **Top Secret**

In addition to these four basic classifications there are additional qualifiers that can be applied to further restrict access. These include:

- **LIMDIS**—Limited Dissemination
- **Special Access Program (SAP)**—Each of which is assigned a Code Word or Nickname
- **Extremely Sensitive Information**—Information and material related to the Single Integrated Operational Plan for the conduct of nuclear warfighting operations.
- **Sensitive Compartmented Information (SCI)**—This category requires special controls with Code Word compartmentalization.

In addition, other restrictive markings and controls can be placed on documents and information. These include:

- **ORCON**—Originator controlled dissemination and extraction
- **WNINTEL**—Warning Notice, Intelligence Sources and Methods
- **NOFORN**—Not releasable to foreign nationals
- **NOCONTRACT**—Not releasable to government contractors

The system has been in place since the Eisenhower Administration and the quantity of classified material, and the duration that it must remain classified has grown significantly and made the management of sensitive information into a behemoth. Important information cannot be made available and sensitive information is not being protected. Classifications are assigned subjectively and inconsistently. [6] If this overview of the Collateral National Security Information system has left you confused, then you are in good company because many within the military, and most of the civilian agencies who need to share their data are too.

***Civilian Classifications***
Governmental agencies such as the CIA use the same basic tier system for classification, but layer on additional markings such as Director of Central Intelligence Sensitive Compartmented Information Programs (DCI SCI). [6]. There is currently little or no capability in place for intelligence and law enforcement agencies to access information stored in military databases, nor is there any capability for these agencies to

share data. One glaring problem is a parochial desire to protect "turf" that is so ingrained that it has become a part of the corporate culture. [3]

***Training and User Friendliness***

Databases that are used by law enforcement and intelligence services must be user friendly and the users must have sufficient training. The Automated Case Support System (ACS) used by the FBI is an excellent example of failure on both these points. A failure in training on how to use this system on the part of agents classifying information led to the success of Robert Hanssen, a highly placed double-agent in the FBI.

A commission investigating the Hanssen case reported, "It does not appear that Hanssen possessed system administrator access or that he hacked into any files." Because ACS is so difficult to use, and agents so poorly trained, they simply didn't bother to restrict files. "Many, particularly at headquarters, are unaware that the restriction capability even exists," the report stated. [4]

## Enabling Technologies

In order to create a collaborative information sharing environment that can be effectively used by all agencies and offices involved in the intelligence and law enforcement community, a number of cyber-security issues must be addressed. There are several technologies that are either currently available or in final development stages that can be used for this effort.

***Intrusion Detection***

Intrusion Detection is one of the cornerstones of cyber-security. It is vital to maintain an active security program by following basic principles such as: implementing patches and hot-fixes as they become available; exercising the principle of least privilege among users; implementing and maintaining an anti-virus program; and closing down services and protocols that are not needed for operations. There is however always the possibility that an intruder will get access to the most well protected system. Intrusion detection methods must be implemented; otherwise the successful attacker will never be detected. There are a number of Host Intrusion Detection Systems (HIDs) and Network Intrusion Detection Systems (NIDs) commercially available and they should be examined suitability. Unfortunately, with most environments, the sheer quantity of data, sensor logs, and audit reports make it impossible for a human to perform correlation and analysis.

The Intelligent Agent Security Module (IASM) is a tool being developed through a government program called Small Business Innovation Research (SBIR) for the US Navy's Space and Naval Warfare Systems Command (SPAWAR). It is a network sensor fusion tool that is capable of looking at various sensors within a network and detecting malicious activity. The IASM ties into Firewall, Router, VPN, Security Tools, Raw IP traffic, and other sources to more accurately report suspicious activity. The IASM performs correlation, analysis, and assessment, along with generating

conclusions, and providing recommended courses of action (COAs) to the user. A test of the IASM was performed using a 24-hour sample of data from a US Navy protected enclave (LAN). The results were that from 6.5 million data records analyzed by the Cisco Secure IDS (formerly Netranger), a NIDS product currently in use by the Navy, there were 178,800 suspicious events identified. The same data resulted in 190 suspicious events when analyzed by the IASM. Obviously a human cannot investigate 178,800 events per day, but 190 is within the realm of possibility, and the IASM is a system that will learn about the network it is monitoring and become more accurate, quickly reducing the number of false positives. The use of IASM on an information sharing and collaboration effort would provide additional assurance that the network was not compromised.

***Multiple Security Levels (MSL)***

When handling classified information, a computer system is accredited for material of that particular level of security. (i.e. to process, read, write secret material, one needs a computer system that has been certified for "Secret") The handling of Secret material, in the computer world, is strictly controlled and computers or storage media (disks, tapes, etc.) not labeled "secret" cannot come into contact with a Secret system. If they do, they are required to have a complete reformat and hard-disk wipe in accordance with DOD policy.

The implications of this restriction are that a user cannot process secret material, and access the SIPRNET (Secret Internet Protocol Routing Network) on the same computer on which they process unclassified material. The risk is that secret material will be inadvertently released through the unclassified connections to the NIPRNET (Unclassified but Sensitive Internet Protocol Router Network). From a functionality standpoint, this makes it very challenging to collate data that may come from different sources, carry different security classifications, including open-source (newspapers, television, etc.) into a cohesive, usable form.

MSL is an interim solution that has been developed by the United States Navy that provides a number of capabilities addressing the need to work with information of different security levels. Currently, a device is available that can allow work to take place with both Secret and Unclassified data simultaneously through the use of multiple windows.

MSL is considered an interim solution until a capability known as Multiple Level Security (MLS) is introduced. This capability has been in development by the military for many years now and the challenges that the product must overcome before it can be used are too numerous to be discussed here.

***Coalition WAN***

Beyond the challenge faced by the developers of MSL is the need to share classified data with our strategic partners such as fellow North Atlantic Treaty Organization (NATO) members. Coalition WAN is the capability of US forces to share strategic and operational data with coalition partners.

The United States, United Kingdom, Canada, Australia, France, and Germany are in the process of deploying computer terminals that will be dedicated to planning coalition operations. These terminals will be used to plan coalition operations, but a six-unit deployment is a very small step towards the level of interconnectivity and bandwidth sharing that is required. Before operational Coalition WAN can be achieved, a number of problems must be solved including bandwidth limitations, language barriers, and an inherent unwillingness to share information, even with long-time allies. [7]

This initiative is a significant step forward, but does not solve the problem of a reluctance to share data that can benefit coalition operations. According to Donald Henry, Special Assistant to the Director of Net Assessment within the Office of the Secretary of Defense, "99 percent of SIPRNET (U.S. Secret Internet Protocol Router Network) is releasable to allies." [7]

When solved, the Coalition WAN technology can be leveraged to permit the sharing of law enforcement data. For suspected terrorists and other international criminals to be apprehended in a world of jet travel and relaxed borders, the United States and other law-abiding countries must share data.

***Virtual Private Networks***

Virtual Private Networks (VPNs) provide several capabilities to agencies active in Homeland Defense. The majority of the internet is operated and maintained by private industry and is inherently insecure. Data packets can be intercepted, sending and receiving computer identities can be detected and "spoofed", and any communications or data transmitted via the internet is open to be read by all.

VPNs provide a secure tunnel through which encrypted data can be sent and received. They provide a level of assurance that allows protected LANs to communicate securely with one another over the unsecure medium of the internet.

For organizations to share vital and potentially sensitive data with one another the use of a VPN is a proven, widely accepted, and reasonably priced solution. For example, if the FBI wanted to provide access to certain databases for local law enforcement agencies to access for performing checks on possible terrorists, the use of a VPN between the LEA and the FBI database would almost certainly be used. A VPN would provide the level of information security required for the sharing of sensitive data.

***Public Key Infrastructure***

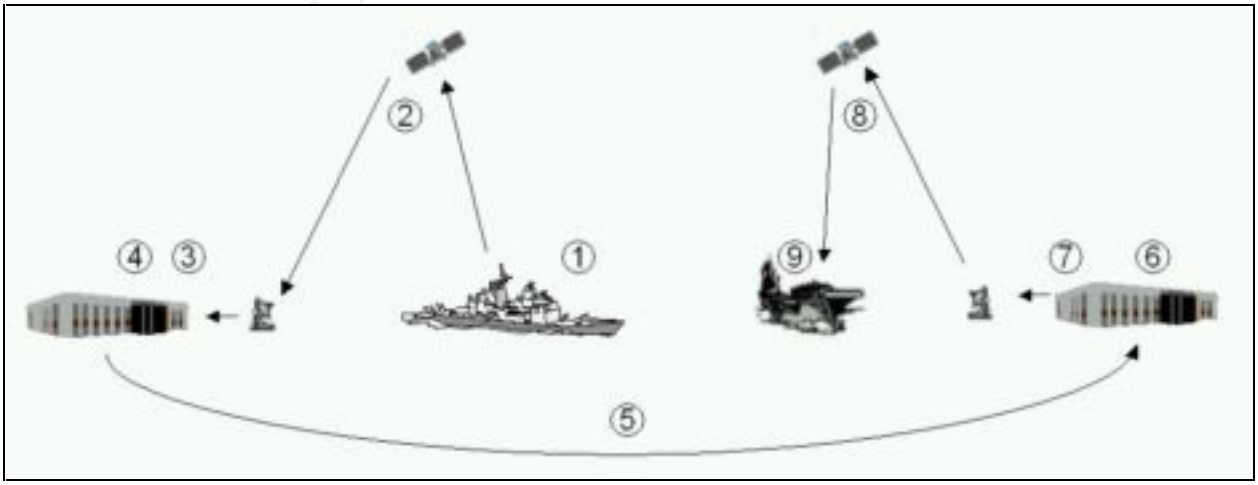
Public Key Infrastructure (PKI) is a technology that enables the degree of data sharing that is required to combat terrorism both domestically and abroad, in unilateral and multilateral efforts. PKI, or asymmetric key, is an extremely secure method of ensuring that communication has security, authentication, non-repudiation, and integrity. It is, unfortunately too slow for use in dynamic environments where encryption and decryption must take place "on the fly" such as voice, video, and streaming data communications.

In order to communicate at voice, video, and streaming data speeds, symmetric key—also referred to by the US military as "traditional key" must be used. In order for two devices to communicate with one another using traditional key, both devices must be loaded with the same key (hence the term symmetric). Traditional key material requires distribution, inventory management, and in most cases, manual loading into the secure communications device. The process requires an extensive infrastructure to assure the security of the key while it is distributed and stored, and an extensive management system in order to keep elements that need to communicate with one another "on the same key". In addition, if a communications device loaded with key is captured then all devices using that key must "re-key" in order to maintain secure communications.

PKI offers an alternative to the traditional key management and distribution system. A new generation of communications devices can be created that will internally generate their own traditional key and use PKI to exchange that key with a device with which it needs to establish communications.

As an example of a situation that would benefit by using asymmetric key to exchange symmetric key: In certain cases US Navy units within the same satellite footprint are unable to communicate using a direct hop, over a satellite, to the destination vessel (on an encrypted channel). The two vessels could even be within sight of one another. This is because, by virtue of how the units are organized hierarchically, they may not have the same symmetric key. In this scenario the message travels on this path:

1. Message is encrypted.
2. It is sent via satellite to the Fleet Network Operations Center (NOC)
3. Message is decrypted.
4. Message re-encrypted by the NOC (using a different key).
5. Transmitted by VPN to the Fleet NOC the recipient vessel is currently logged into.
6. NOC decrypts the message.
7. The message is re-encrypted with the key that the destination vessel is using.
8. Message transmitted via satellite to the intended recipient.
9. Recipient decrypts the message.



By using PKI to exchange symmetric key the two vessels could eliminate a significant part of this information overhead. A similar scenario might happen when two army units wish to talk over secure voice communications, but do not have the same symmetric key or when a CIA agent wishes to establish a dial-up connection to a central information database to input new information or search for data.
Use of PKI by units in the field, be they agents or military units is an enabler that will allow the United States to project its information power not unlike power projection from a traditional military perspective.

***Common Access Card***
The Common Access Card (CAC) is in conjunction with PKI deployment to provide an even greater level of information assurance. A CAC card has an embedded chip that has information allowing the owner to encrypt and decrypt messages. The CAC alone is not sufficient, but must be coupled with a password in order to operate. CAC cards coupled with PKI provide authentication, security, integrity, and non-repudiation to a very high degree. The DOD is currently in the process of deploying CAC cards to 3.5 million personnel. [9]

**Initiatives**

***International Networking***
In November 2001 the United States awarded a contract to Anteon International, Inc. to develop a global network for non-NATO allies to share intelligence in the war on terrorism. According to the Pentagon, Al Qaeda has operational terrorist cells in between 50 and 60 countries around the world. [8] Anteon currently has a five-year $100 million contract to upgrade the existing NATO systems.

***Data Fusion***
A Data Fusion Center to serve as a central repository and data warehouse for the intelligence agencies has been discussed by lawmakers. This Defense Advanced Research Projects Agency (DARPA) is in the process of putting together a prototype National Data Fusion Center (NDFC) for intelligence agencies to share both classified and unclassified data. [5] The concept behind this initiative is to develop a database interconnection that will allow participant agencies to pull data from other repositories such as the FBI and CIA. The National Data Fusion Center would then maintain the database connectivity and provide tools for interested parties to search and retrieve information.

The cyber-security challenges that face the NDFC are identical to those that face any intelligence or law enforcement agency in trying to make data accessible to partner agencies that need it. Correlating security levels of the information, keeping the different levels of information separate, and querying parties will still need to use machines certified for the security level of the information,

***Data Mining***
The ability of a U.S. Army Military Intelligence unit to provide a detailed eight-page briefing on subjects that the CIA were only able to develop two lines of information for (described above) can be credited in large part to advanced data-mining tools to extract required information from a virtual ocean of data. [5] The use of such tools by all agencies is vital for information operations.

## The Future

To truly solve the problem with data sharing, data mining, and the conflicting classifications of sensitive documents will require the creation of a new entry, storage, and retrieval system.

According to FBI Director Mueller, what is needed is "substantially greater and more centralized analytic capability resident at [FBI] headquarters, but available anywhere in the world" and that the Bureau also needs to be "better intertwined with other agencies" so they can share information. [2]

The time has come for the President to order the development of a National Intelligence and Law Enforcement System. Such a system would require, at a minimum, the following characteristics:

1. The establishment of a standardized data set. While certain types of reports and data entry will not be pertinent to all agencies using the database there are many that are. The development of common and agency specific data fields will be one of the most challenging but vital milestones to meet in this project.
2. A nationally applied security classification system. The Collateral National Security Information system needs to be overhauled and streamlined. Classifications must be clearly defined and their use mandated for all agencies. Without establishing this common system, the new system cannot be administered because the assignment of privileges to users will be rendered subjective by the inconsistency of the material they attempt to access.
3. Robust and configurable data mining tools. Commercial off-the-shelf (COTS) tools currently in use will be required for law enforcement personnel accessing the new database to be able to “sift” through the veritable ocean of data. Standard search tools can be created and available based on the user profile of the accessing agencies. (i.e. a set of tools for local police, a similar, but different set for FBI offices, etc.)
4. Effective intrusion detection, system monitoring, firewall, and anti-virus capabilities. By consolidating vital intelligence data there are benefits of economy of scale, elimination of redundancy, and consolidated management. Conversely there is increased risk because hackers, both individual and state-sponsored have a single point of focus for their malicious efforts.

5. The development of a manageable and effective secure access coupled with proper training. By making the new database available to offices such as state and local law enforcement there are a number of new issues that must be addressed. First, a large number of individuals will require a National Agency Check (NAC) and the grant of a security clearance. Cleared individuals then will need to be processed for access to the new system, their logon, password, and access level created and distributed to them. To ensure a high level of security the use of a Common Access Card (CAC) or biometric identity verification for access to the database could be required. All users of the system must be properly trained in its use in order to prevent unauthorized access to sensitive data.
6. Multi-Level Security issues must be solved. The capability for a terminal to provide access to sensitive material at the level it is certified for as well as all material holding lower level classification is imperative. In order for law enforcement to be effective they cannot be expected to research the same subject multiple times from multiple computers.
7. Extensive and thorough backups and redundant systems. A tool with as many users as this new database will need an extremely high availability rate. Only by maintaining complete backups and perhaps the maintenance of a backup site will the required service level be assured.

The United States is the most prosperous nation in the world, but we do not have the luxury of supporting several dozen independently operating intelligence and law enforcement agencies. Intelligence gathering, data storage and mining, and cyber-security has matured to a level that will support consolidating the majority of these efforts. Such a consolidation will provide a number of benefits to the United States. There will be considerable cost savings by eliminating redundant agencies and support systems that are duplicated within each agency and office. The responsiveness of the system will allow the currently reduced number of law enforcement and military personnel to be more agile and effective. Finally, it will provide a quantum leap for US agencies leading to the detection and apprehension of not only terrorists, but also other threats to our nation, people, and national interests.

**Bibliography**


1. Jackson, William. "Senate committee set to act on cybersecurity bills" *Government Computer News,* May 20, 2002 URL: http://www.gcn.com/21_11/homeland/18656-1.html

2. Matthews, William. "FBI Counting On IT vs. Terrorism" *Federal Computer Week, May 20, 2002 URL:* http://www.fcw.com/fcw/articles/2002/0520/web-fbi-05-20-02.asp

3. Dorobek, Christopher. "Intelligence Info Sharing 'Inept'." *Federal Computer Week,* May 27, 2002. URL: http://www.fcw.com/fcw/articles/2002/0520/web-info-05-24-02.asp

4. Jackson, William. "Cyber Eye: The trick to security: Make it easy." *Government Computer News.* May 20, 2002 URL: http://www.gcn.com/21_11/homeland/18648-1.html

5. Shiral, Maureen. "Key Lawmaker Laments Lack Of Intelligence Info-Sharing System" *GovExec.com,* May 23, 2002 URL: http://www.govexec.com/dailyfed/0502/052302td2.htm

6. Pike, John. "Security and Classification." 1998. URL: http://www.ostgate.com/classification.html

7. Caterinicchia, Dan. "NATO Terminals Link Allies" *Federal Computer Week*, May 27, 2002 URL: http://www.fcw.com/fcw/articles/2002/0520/web-nato-05-24-02.asp

8. Capaccio, Tony. "U.S. Sets Up Terror Intelligence Network With Non-NATO Allies." *Bloomberg.* May 20, 2002 URL: http://quote.bloomberg.com/fgcgi.cgi?T=uspolitics_news.ht&s=APOlauBUjVS5TLiBT

9. Dorobek, Christopher. "DOD delays smart card deadline." Federal Computer Week, February 7, 2002 URL: http://www.fcw.com/fcw/articles/2002/0204/web-cac-02-07-02.asp