

A White Paper:

Department of Homeland Security Information Assurance Issues and Possible Solutions

PREPARED FOR:

Department of Homeland Security and Its' Agencies

Contact:

DigitalNet
2525 Network Place
Herndon, VA 20171

703.563.7500
www.digitalnet.com

This White Paper includes data that shall not be disclosed outside the Government and shall not be duplicated, used, or disclosed—in whole or in part—for any purpose other than to evaluate this White Paper. If, however, a contract is awarded to this offeror or quoter as a result of—or in connection with—the submission of this data, the Government shall have the right to duplicate, use, or disclose the data to the extent provided in the resulting contract. This restriction does not limit the Government's right to use information contained in this data if it is obtained from another source without restriction. The data subject to this restriction are contained in sheets marked with the following legend: "Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this White Paper."

Contents

Section 1 — Introduction.....	1
1.1 High Assurance Security Protection for the DHS.....	1
1.2 TEMPEST/Zone.....	2
Section 2 — ESS Operational Risk Issues.....	3
2.1 Operational Security Issues — Directory Interfacing and Data Sharing.....	3
2.2 Operation Security Issues — Sharing of “Releasable” Data	4
2.3 Cryptographic Interoperability Issues — Exchange of Information between Enclaves Using Different Encryption Technologies.....	4
2.4 Operation Security Risks — Electronic Emissions.....	4
Section 3 — Recommended Solutions for DHS Operational Risks.....	6
3.1 High Assurance Security Protection for the DHS.....	6
3.1.1 Concept of “DHS Perimeter Protection Services”	8
3.1.2 Network Guard Functions	10
3.1.3 Inter-Agency Releasability Functions.....	10
3.1.4 Mandatory Audit Functions	11
3.1.5 “Border Directory” Functions.....	11
3.1.6 Cryptographic Interoperability Concepts.....	12
3.1.7 Security Management and Control Concepts.....	13
3.1.8 Trusted Access Using the Secure Dual-Mode Workstation.....	13
3.2 TEMPEST/Zone.....	15
3.2.1 TEMPEST/Zone Options for the DHS System Environment.....	17

Section 4 — DigitalNet Related Experience..... 19

4.1 DII and DMS Guard Program..... 19

4.2 DISA Command and Control Guard System 19

4.3 DataSync Guard System..... 20

4.4 FBI “Cyclone” Network Guard Program..... 20

4.5 Department of State Telegram Distribution Guard Program 20

Section 5 — Recommendations..... 22

5.1 Guard Technology..... 22

5.2 TEMPEST/Zone Technology..... 22

List of Figures

Figure 3-1. DHS Shared Infrastructure Concept..... 7

Figure 3-2. Security Policy 9

Figure 3-3. Trusted Access System..... 14

List of Tables

Table 3-A. DigitalNets Offers Solutions to Counter the Main Risks 6

Graphics

Explanation of acquisitions to create DigitalNet.....24

Department of Homeland Security Information Assurances Issues and Solutions

Section 1 — Introduction

DigitalNet is pleased to offer these possible information assurance solutions to the DHS. DigitalNet, formerly Getronics Government Solutions, is a full service systems integrator focused on developing and providing secure networked solutions and services for the federal market. We have organized our white paper as follows:

- Section 1 provides a brief introduction.
- Section 2 describes the major operational risks the DHS program will face.
- Section 3 offers potential solutions for high assurance security protection issues (including a potential DHS topology concept) as well as TEMPEST/Zone solutions.
- Section 4 presents some of our additional qualifications in this area.
- Section 5 presents our recommendations for the final DHS RFP.

As part of our commitment to our customers we have developed two technologies that we feel have a place in the DHS, High Assurance Security Protection and TEMPEST/Zone.

1.1 High Assurance Security Protection for the Department of Homeland Security

For many years the Intelligence Community has been faced with information sharing challenges that most civilian agencies have not had to face until now. However, as civilian agencies become more committed to share information, in an effort to secure our borders, they will be faced with similar challenges already encountered and addressed by the Intelligence Community.

For example, we anticipate that civilian agencies will face the challenge, previously addressed within the Intelligence Community, of how to share information across networks operating at different classification levels, such as Top Secret versus Sensitive but Unclassified. In fact, we believe that this challenge will have to be confronted during the design of the DHS network with respect to both inter as well as intra-agency communications.

The DHS information-sharing problem will be compounded several fold because of the need to: (1) integrate existing applications and networks within the DHS design, and (2) implement DHS quickly. These existing networks and applications were never designed to work in a cooperative environment but were designed as “point solutions” to manage a specific application within a specific agency. That agency had complete control over who used the networks and data. Now, all appropriate Government applications will become a subset of the “virtual” DHS database. The challenge will be to “protect and share” at the same time. In addition, DHS will not have the luxury of time to test unproven and untrusted information sharing technology.

DigitalNet has been providing National Security Agency (NSA) certified information sharing

technology for similar networks and applications for more than 10 years with over 275 of these systems currently in production protecting some of the most sensitive information that can be found in the U.S. Government. Without these systems, the Intelligence Community would be unable to function efficiently.

In many cases within the civilian government agencies security has been an issue that has been considered something that constrains the mission of the agency. However, these technologies addressed in this paper, are “enabling” technologies because the agency mission, in many cases, could not be accomplished without them.

1.2 TEMPEST/Zone

The DHS will also encounter other issues that have faced the Intelligence Community for many years. Often times, the Intelligence Community does not have complete control over a physical environment where electronic data must be created, processed, and stored. Those physical locations can be either in the U.S or outside our national boundaries. The community has long known that with a couple of hundred dollars worth of inexpensive electronics, the “bad guys” have the ability to “see” what is on computer monitors, disk drives, and electrical wire of COTS office automation products such as PCs, servers, switches, routers, etc. Those that wish to do us harm do not need to steal data while it is in transmission over the network. They can steal that information as it is being created or displayed because of the electronic emanations those COTS devices produce.

The DHS will have similar issues with which to contend. For example, Government or contract employees located at an airport or port-of-entry will require access to the “virtual” DHS database to perform their jobs. As that individual queries the DHS database, the query response is protected by the finest network security technology available today as it traverses the DHS network in an encrypted state to the endpoint, which may be a networked PC or a networked printer in an airport in a public area. At the endpoint at the airport, the information is de-encrypted and is displayed or printed by COTS devices (PCs, printers, switches, copiers, etc.). Unfortunately, those devices are “broadcasting” for anyone to intercept the type of information that is stored on the DHS network.

DigitalNet has been designing and building TEMPEST/Zone technology for more than 22 years that eliminates this problem for those users who need to eliminate emanations coming from COTS tools that are critical to successfully performing their mission.

After reading our response, we hope that you will consider these issues that we have raised and incorporate the benefits of this technology in the DHS.

Section 2 — DHS Operational Risk Issues

From our understanding of the requirements for the DHS, it is very important that the DHS be protected from unauthorized data access and tampering from threats that may exist external to the system or within the DHS itself. If the DHS data can be accessed or tampered with by unauthorized persons then not only is the entire value of the system destroyed, but significant legal liabilities may arise. The integrity of the DHS data collected by the remote DHS collection agencies must be ensured as that data is passed on to the central DHS databases and analysis systems. This requirement for high levels of security and integrity of the system leads to some significant operational issues since the design of the DHS network will almost certainly involve a distributed network-centric architecture incorporating a central DHS database and management system node with a variety of different remote DHS data collection sources. The design of the network will almost certainly also involve other agency participants as well as including a variety of other authorized external users. It is expected that all of these authorized DHS participants will interact using the connectivity provided by existing and available common user networks such as the NIPRNET or equivalent Government-provided networks. From a cost viewpoint, it is crucial to consider the utilization of the totally unprotected internet as the connectivity backbone for the system. Since these networks are used by a large number of other non-DHS users, and it must be assumed that they will certainly not be highly secure, the DHS system architecture must be developed so that it can provide its own highly protective security domain which can be easily extensible to encompass all authorized participants in the DHS as they vary over time.

There are four major operational security risks that will be discussed in more detail in the following sections:

- Directory Interfacing and Data Sharing
- Sharing of Releasable Data
- Cryptographic Interoperability
- Electronic Emissions

2.1 Operational Security Issues — Directory Interfacing and Data Sharing

Directories are used to store important information that must be shared by a widely distributed community of interest. The type of information stored in a directory may include individual and organizational names, network addresses, individual and organizational security certificates, and data and communication access permissions. Assuming the DHS will require interagency communications, a directory will be required to locate individual and organizational names, addresses, and access permissions for various agencies participating in DHS.

Because of the range of services to be supported by this directory, it is assumed that this will be an X.500 Directory implementation. A DHS Directory could be provided as a stand-alone Directory, which is maintained and updated directly as changes are required/occur. It could also be automatically updated from the directories currently maintained by the various DHS

participating agencies for their own internal use. To eliminate redundant labor-intensive efforts and data synchronization issues as well as to ensure the security and integrity of the DHS directory subsystem, the second alternative is recommended using a directory transaction guard system similar to those provided by DigitalNet on other programs such as DMS.

2.2 Operation Security Issues — Sharing of “Releasable” Data

Based upon our previous experience on the DoD Command and Control Guard Program, the FBI Network Guard Program, and the Defense Message System Program, there will ultimately be an operational requirement for different agencies to exchange certain types of authorized “releasable” data and messages to the DHS and visa-versa. As an example, this is already the case in our work with the FBI for which certain types of data are securely exchanged between FBI and the U.S. Customs Agency or between FBI and the U.S. Department of Treasury under very controlled conditions of automated content release review and authentication of sender/recipient authorizations. We believe that the willingness of other agencies to participate with the DHS will be limited unless the DHS operational concepts are extended to include the secure, controlled release and exchange of authorized data between different agencies. To accomplish this with high assurance security protections, the DHS should incorporate and build upon the network releasability Guard technology, which has already been developed, accredited, and utilized by the DoD and other agencies including FBI, DEA, and Department of State.

2.3 Cryptographic Interoperability Issues — Exchange of Information between Enclaves Using Different Encryption Technologies

The DHS may require the interchange of sensitive information usually protected by data encryption methods. Different agencies often employ differing encryption methods and algorithms to protect their sensitive information. In order to share such information, it must be decrypted from the agency-particular standard and re-encrypted to a form acceptable to the target enclave. This may be an operational issue depending upon the sensitivity of some of the information to be exchanged between the DHS and participating agencies.

2.4 Operation Security Risks — Electronic Emissions

When people talk about computer security, they most commonly focus on that aspect of computer security associated with the use of passwords, encryption and firewall techniques. Many people are not aware that information being processed on commercial equipment – desktop computers, laptops, printers, scanners, switches, and the like – can be readily and easily compromised through the use of equipment that can be purchased at most electronics stores.

Standard electronic equipment emits electronic and electromagnetic radiation either through the air or through conductors, such as the AC wiring in a building. Such emissions can be intercepted and analyzed, allowing eavesdroppers access to sensitive information. Data processed by commercial equipment can be detected by monitoring equipment located in a van that is parked, for example, outside a non-secure building. A non-secure building is one that lacks shielding that prevents emissions from radiating to the outside world, thereby divulging the information being processed by the computers and associated peripherals that are in use at the

time. Eavesdroppers do not have to invade the premises or access telephone lines nor do they need a password to get into a system. Surveillance of this nature can occur without the knowledge of whoever is being targeted by an eavesdropper.

What does this mean, then, for Border Guards, the State Police, Local Police, Airport Authorities, etc. and those responsible for our Ports of Entry who occupy buildings that are not shielded? It means that potential eavesdroppers can easily capture the electronic emissions from information processing equipment in use at the time and that the information that is intercepted can be then used against U.S. interests.

Section 3 — Recommended Solutions for the DHS Operational Risks

DigitalNet recommends two solutions (Table 3-A) to counter the four major risk areas discussed in Section 2. Sections 3.1 and 3.2 will discuss the aspects of these solutions in depth.

Table 3-A. DigitalNet Offers Solutions to Counter the Main Risks

Risk	Solution
Directory Interfacing and Data Sharing	High Assurance Security Protection
Sharing of Releasable Data	
Cryptographic Interoperability	
Electronic Emissions	TEMPEST/Zone

Section 3.1 describes how the Guard could be used to mitigate the directory interfacing and data sharing risks, sharing of releasable data risks, and cryptographic interoperability risks. The Guard technology can be architected so that a single system can manage multiple risks.

3.1 High Assurance Security Protection for the DHS

Figure 3-1 provides a simple notional illustration of what might be involved in the DHS operational topology. To provide for the operational security and integrity of the DHS network it will be necessary to first of all ensure that the DHS’s central database is only accessible by authorized individuals or processes for purposes of either querying or updating the database. It will also be important to ensure that only authorized individuals have access to the DHS system management and analysis tools as well as to the DHS system security management tools. Since there may be different individuals from different organizations, each with differing levels of access authorization and trust, it will be necessary to not only ensure that individuals (processes) are authorized for access, but it will also be necessary to ensure that the transactions undertaken are strictly within the authorized security and integrity profiles established for those individuals (processes). In other words, to adequately protect the DHS database(s) and other system functions it will be necessary to not only verify a user’s identity and authorization profile, but also to perform checks on the actual transactions that the user attempts in order to ensure that they are within his or her allowed authorization profile.

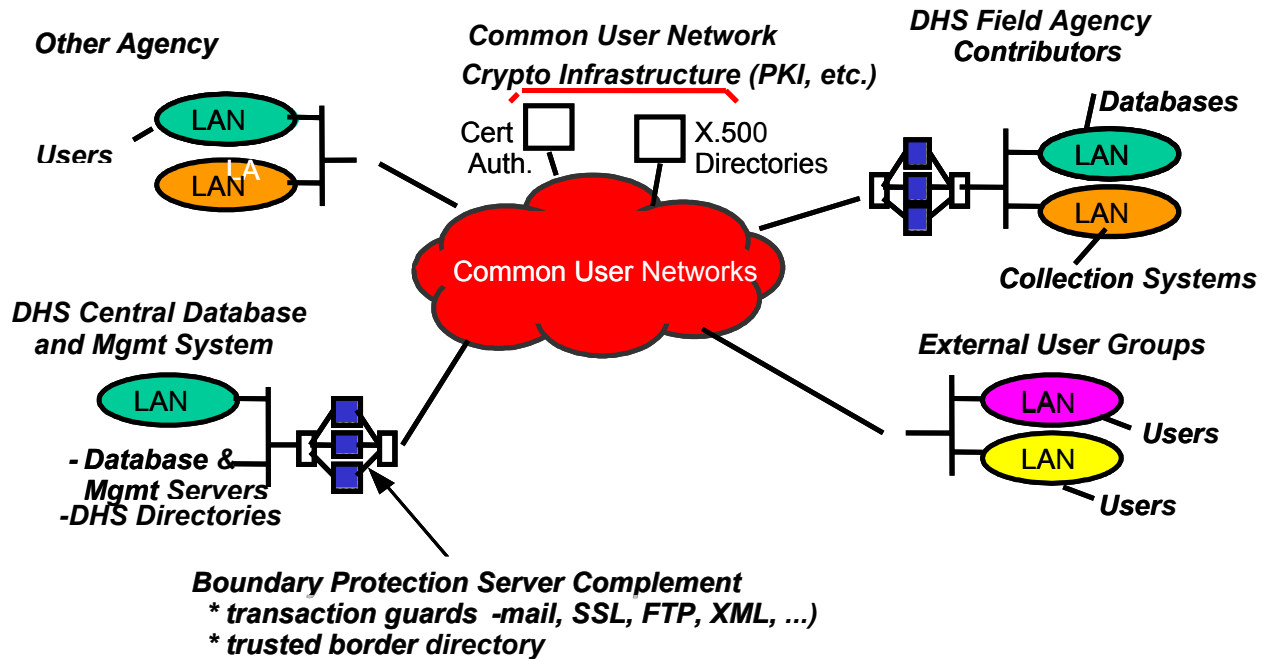


Figure 3-1. DHS Shared Infrastructure Concept

In developing the DHS architecture and implementation design, it will be required that the database management products and application software utilized be standard, commercially available products that utilize standard database interface transaction protocols. This will be necessary not only from a system lifecycle cost point of view but also since the DHS database management systems will be required to interface with a variety of standard commercial systems already deployed and maintained by other agencies or programs. Unfortunately, none of these commercial database system products incorporate the level of self-protecting security functionality necessary to protect them from being successfully attacked and compromised by knowledgeable system hackers. For this reason, we believe that the DHS database system architecture should incorporate the use of high assurance network guards of the type used by DoD and the Defense Information infrastructure for purposes of providing a very strong perimeter of security protection around the core of the DHS. These types of perimeter guards are capable of protecting themselves from penetration and compromise while enforcing the various specific access control and security monitoring and filtering policies necessary to protect the DHS infrastructure. A notional illustration of where these guard systems might be used is illustrated in Figure 3-1.

DigitalNet currently builds and deploys a variety of high assurance network transaction guards including various e-mail guards, database transaction guards, file transfer guards, directory transaction guards, and Web-based guard systems. Many versions of these products have been accredited and certified for operation by the Department of Defense and by several intelligence agencies. Some of the most notable of these include the U.S. Defense Information Infrastructure

(DII) e-mail and directory guard system now being fielded as part of the U.S. Defense Messaging System (DMS). Others include the DoD Standard Command and Control Guard (C²G) system currently fielded by the Defense Information Systems Agency (DISA), the high assurance network Guard systems now deployed by FBI, and the Data Synchronization Guard (DSG) system recently accredited by NSA and the DISN Security Accreditation Working Group (DSAWG) for use by the U.S. Army.

In addition to high assurance network security Guard technology, a necessary part of the DHS security architecture will include the use of cryptographic protections for DHS-related network transactions. This will be necessary since DHS will undoubtedly make use of relatively unprotected and untrusted common user networks to support the required connectivity between data collection functions, central database and management functions and a variety of different internal and external users. To accomplish this, a number of options exist for the use of existing “public key” cryptographic infrastructures (PKI), which already have been fielded particularly as regards the U.S. Government supported networks (DISNs). DigitalNet has a great deal of experience in the design and utilization of public key cryptographic infrastructures (PKI) as well as the design of the supporting directory systems which would be necessary to implement in support of the DHS system. Also, DigitalNet’s high assurance network transaction guards are interfactable with most commercially available PKI and other cryptographic technologies such as secure socket layer (SSL) security mechanizations. Additionally, the use of PKI-type network encryption technology not only provides confidentiality and integrity protections for transaction data “in transit” across the network, but also provides very strong identification, authentication, and non-repudiation functions for users (processes) attempting to conduct transactions with the DHS. With this capability, the secure perimeter protection concepts previously discussed are completely compatible with standard network encryption protections.

3.1.1 Concept of “DHS Perimeter Protection Services”

Figure 3-2 illustrates a notional concept of the DHS infrastructure including its interfaces with common user supporting networks and with external participating agencies and other users. Our concept for high assurance “DHS Perimeter Protection Services” would center upon the use of a basic complement of high assurance security enforcement servers as shown in Figure 3-2. The following sections describe the three servers in more detail.

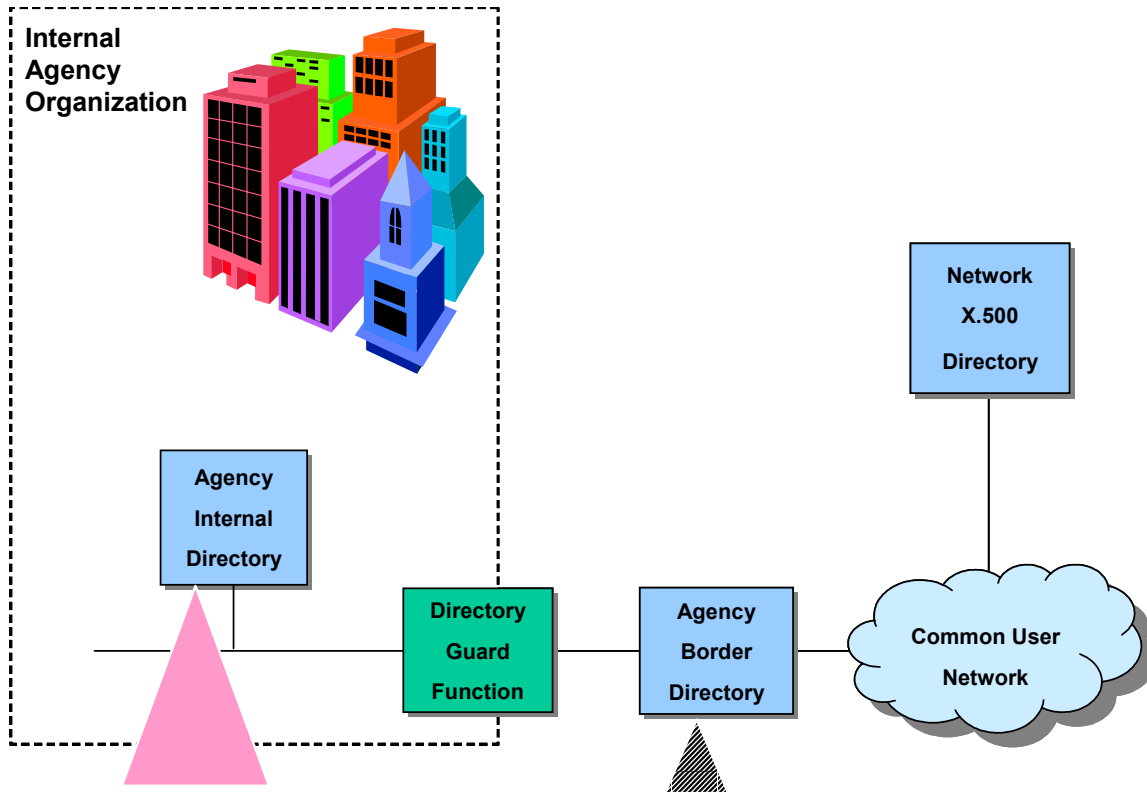


Figure 3-2. Security Policy

3.1.1.1 Agency Internal Directory

The first of these servers would be used to implement e-mail Guard security services and would provide support for the appropriate network encryption services for both the DHS infrastructure and for the participating agency's selected internal encryption infrastructure, if it is in fact different. We would expect that the primary e-mail service provided would be SMTP; however, X.400 e-mail services could also be provided simultaneously, if required. This e-mail Guard has already been developed and accredited by DigitalNet and NSA (the installed base is 240 Guards with more installed each month) and is capable of interfacing directly with the Agency's local e-mail message systems, such as Microsoft Outlook.

3.1.1.2 Data Synch Guard

The second server in the basic Perimeter Protection complement would be used to implement a variation of DigitalNet's current DataSync Guard system, which would provide security functions as required to authenticate and mediate network services including FTP, HTTP, and a variety of socket-to-socket-based transactions, which would include such things as SQL database transactions, as well as providing authentication and session connection services for voice-over-IP and video-over-IP transactions if required. DataSync Guards have been installed in an Intelligence agency and in the Army, and NSA has recently successfully evaluated and approved this product.

3.1.1.3 Border Directory Guard

The third server in the complement would be a Border Directory Server, which would provide

for the secure sharing of authorized and releasable internal directory information across the DHS infrastructure and whose functions are described separately in Section 3.1.5.

As with the e-mail Guard server, both the Border Directory server and the DataSync Guard server would also provide support for the network encryption services for both the DHS and the various participating Agency's infrastructures as required. All of the high assurance Guard systems currently developed and operationally deployed by DigitalNet use 100 Base-T Fast Ethernet for each network connection, and a single Guard system typically comes configured to support nominally four network connections that can be assigned different security levels as required. The number of Perimeter Protection Server complements implemented at a particular site would be scaled depending upon the data throughput and traffic requirements of the site.

3.1.2 Network Guard Functions

As was stated earlier, one of the most important aspects of DHS security concept will be in the access control and in the security review and management of transactions between DHS and the existing infrastructures of the various participating agencies. Without the use of some form of network boundary protection services, the ultimate security of DHS will be dependent upon individual external agency's personnel security policies and the security controls and protections, if any, implemented by that agency including any of its component elements, such as desktop PCs, un-trusted multi-use servers, and any remotely connected devices or network elements. For this reason we believe that, as with SIPRNET/NIPRNET operations, it is necessary that the DHS concept include boundary protection services. NSA accredited network Guard technology should be used for purposes of enforcing mandatory access controls to allow access and use of the DHS services. This type of high assurance access control is usually done using encryption-based identification and authentication (I&A) techniques, such as digital signatures for both individual users and for authorized endpoint processes such as database replication or query processes.

If an agency has already established a PKI or other I&A infrastructure for its internal use then it would be completely feasible for the DHS boundary protection Guard systems to be configured to support that same I&A infrastructure for its local area access control. If required, this network Guard technology could also control, in a mandatory sense, the specific types of network services that were permitted on a user-by-user or process-by-process basis for further security control. In addition, these types of guards are typically configured, as required, to provide automated security review of transaction content for a variety of different services including e-mail, file transfers, and various socket-based transactions. The security filtering involved could include such functions as virus scanning, data format checking, "dirty word" and mobile code detection as well as other filtering functions. This further ensures that authorized users and processes would in fact use the DHS services allowable within their authorized use profile. Finally, network Guard systems are also used to provide mandatory, protected audit information on all transactions for later analysis as required.

3.1.3 Inter-Agency Releasability Functions

In order to meet real operational requirements for the controlled release of authorized data between different subscriber agencies or between different protected domains within a single

agency, each of the three Boundary Protection Servers can be configured to support the cryptographic services necessary to establish communication sessions on an inter-agency basis.

Because each server utilizes a high assurance trusted computer base, the encryption key information used by the servers is completely protected and isolated from any external users or processes. With this capability to securely communicate between agencies in place, the Guard servers and the border directory servers can then utilize different release policy filters to ensure that only authorized endpoints participate in an inter-agency data session and that the information exchanged is limited only to authorized releasable data. Data review and format checking filters can again be implemented at the application level as required by security release policy in order to further verify that only the appropriate releasable information is actually transferred between the authorized inter-agency endpoints. These filter templates can be preprogrammed and installed on the Guard by an authorized security administrator. Different filter templates can be enforced for different originator/recipient combinations if required. In Section 4, DigitalNet's Related Experience, specific descriptive information has been included that indicates how this type of security filtering and control is implemented for a number of accredited operational Guard systems currently used within the SIPRNET/NIPRNET environment.

3.1.4 Mandatory Audit Functions

The proposed Boundary Protection Server complement would utilize DigitalNet's LINUX compliant high assurance trusted servers, which have a long pedigree of evaluations and certifications by NSA. These servers are capable of protecting all application processes and data executing on the servers and can also be configured to collect and archive as protected audit data any security relevant information required by operational security policy. These protected audit data are collected on a mandatory basis and are critical for being able to track transactions and events, albeit after the fact. The audit collection processes and the audit file data are available only to authorized security administrators and are completely tamper-proof in terms of malicious manipulation by any other user or process.

3.1.5 "Border Directory" Functions

Border Directories allow for a subset of the actual information in an agency or other organization's directory to be accessible by the "outside world." This concept is defined in ACP 133. An organization's internal directory may hold thousands of entries but the organization may only want to share 100 entries with an external participating agency. Border Directories allow the organization to only disclose the entries and the particular attributes that they are willing to share with everyone outside their immediate organization. The DHS security architecture should use border directory concepts similar to this to securely control the specific directory information and directory interface functions that are available to the various participating agencies and users that may be involved in the DHS.

In order to enforce DHS Border Directory security policies, directory Guard control filters would be used to ensure that only authorized directory data from the internal DHS directories was accessed and made available to appropriately authorized participating partners. DigitalNet has implemented and deployed similar directory Guard access and control functions as part of the

DMS and DII Guard programs. The following is a list of filtering options that may be required for the DHS application:

- **Remove Trace Information.** In the event that the organization wants to protect IP addresses and other information about the internal directory system from the outside world, this filter will remove any information about the internal system prior to accessing the external server.
- **Protocol Control.** This filter will control the directory protocols that are allowed to leave the DHS boundary and the protocols that are allowed to access internal agency directories from the DHS world. For example, DHS users may be allowed to chain to a member organization's border directory to get information but policy may be enforced to ensure that no users from the DHS access directory information found in the internal organization's directory.
- **Operation.** This filter can allow or disallow directory operations from entering or exiting the DHS Directory system. For example, users may be allowed to read entries but not modify them.
- **Attribute.** This filter can be used to specify the attributes that a user can request of an external directory or to control the attributes that can be replicated to the outside world. For example, the organization's Enterprise Directory may contain hundreds of attributes while only a select few attributes are ever replicated to the Border Directory.
- **Error Handling.** Rather than returning a security error to a user, this filter option allows the directory to return a service error indicating that the directory is busy or unavailable.
- **Authentication.** This filter can be used to verify that only authenticated users are allowed to enter the internal boundary. The system can be configured to only allow certificate-authenticated users to access boundary information.
- **Replication.** This filter can be used to verify that only information agreed upon in the replication agreement is being replicated from the Internal Directory to the Border Directory and from the Border Directory to the DHS Directory.
- **Change Identity of Originator.** In the event internal agency users cannot be known outside of the agency boundary, this filter is capable of changing the identity of the originator. For example, all requests leaving an agency would come from DHS-USER1.

The directory architects and designers will need to work with the system accreditors to determine security policy. This section is merely included to describe the filtering mechanisms currently available (see Figure 3-2).

Border Directory Synchronization. If a given organization that must connect with the DHS Directory already has a pre-existing Directory that does not exactly match the schema defined by the DHS Directory, a Meta-directory product can be used to equalize the information and provide the filtering to only release the required information. Meta-directory products synchronize with multiple directory repositories to provide a common source of data so that investment in existing directories is not wasted but leveraged to become part of a distributed directory system.

3.1.6 Cryptographic Interoperability Concepts

As described earlier, not all agencies will use the same encryption for all types of data. When

agencies with differing encryption technologies need to communicate, a decryption using the source agency's technology and then a re-encryption using the destination agency's technology must be accomplished. A highly trusted platform should be used to house the decryption and re-encryption functions that will be necessary for DHS. These functions can be incorporated in the Guards that will be used to provide the boundary protection services. For NSA, DigitalNet has developed reference implementation libraries to interface with any given encryption engine. This software can be easily integrated with the Guard Operating System state machine type architecture, which allows the insertion of isolated and protected application modules. With this approach, the DigitalNet-developed encryption implementation libraries can be incorporated as application modules in the Guards, which can then execute decryption via the appropriate engine and then pass control to re-encryption via the corresponding appropriate engine.

3.1.7 Security Management and Control Concepts

We would expect that a DHS security administrator would have responsibility to administer the security filters and access control tables for the Perimeter Protection Servers at each of the locations where access protections for DHS assets are required. The security administration for all of the Perimeter Protection Servers could be done remotely from a single agency physical location if desired or, alternatively, from any of the appropriately authorized DHS remote facilities. The security administration facilities and tools available on the Perimeter Protection Servers would only be available for use by an authorized security administrator based upon a digital signature authentication.

At such time when it is desired to enable the controlled release of authorized data between agencies, it will be necessary for security administrators in each agency to coordinate filter policies and access control tables. It would then be suggested that a separate protected "security administration channel" be made available as an element of the DHS service to allow security administrators to coordinate security release policy filters and to update inter-agency access control tables for releasability purposes as required.

3.1.8 Trusted Access Using the Secure Dual-Mode Workstation

Users often need to share operational information in a timely manner, without compromising the information's confidentiality or integrity. To further complicate matters, some users have different authorizations, reflecting the different operational roles they perform. To do their jobs, they need to access computing resources and networks—remote as well as local—that run at higher classification levels or different "needs to know" from their local network. To date, the only way to satisfy their requirements has been to clutter their desktops with multiple computers and network connections—one at the level of each network to be accessed. The DigitalNet Trusted Access system illustrated in Figure 3-3 solves those problems.

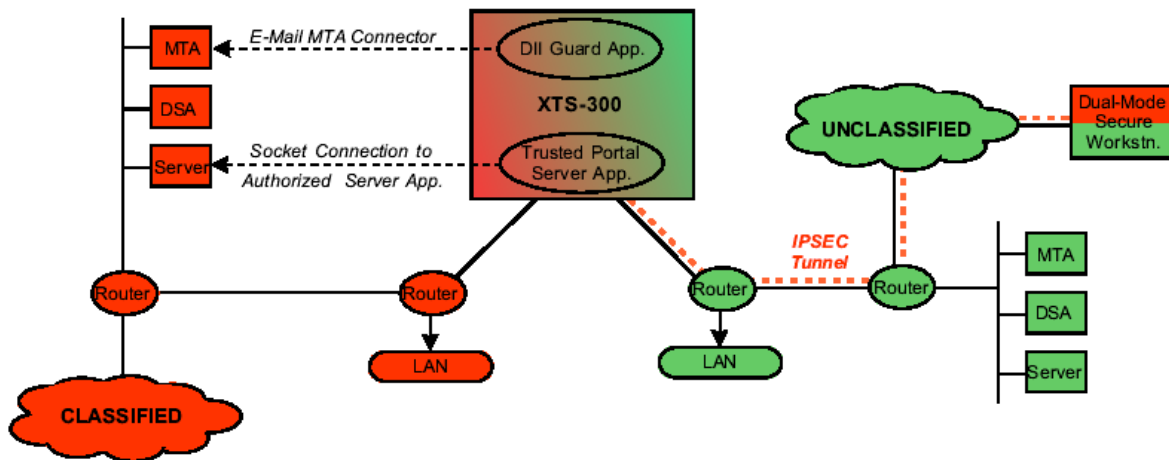


Figure 3-3. Trusted Access System

The Trusted Access System comprises two cooperating components: the Trusted Portal Server application running on DigitalNet’s XTS-300™ NSA B3-evaluated Trusted Computer System and the Dual-Mode Secure Workstation—a high-powered Intel-based workstation with NSA-approved state-of-the-art security technology, including strong authentication, virtual private networking, and mandatory media encryption. The DigitalNet Trusted Portal consolidates the user’s computing and networking resources onto a single desktop, providing a single, secure workstation that can operate at one of two different sensitivity levels at any given time.

The Trusted Portal combines this Dual-Mode Secure Workstation with a high-assurance Trusted Portal Server that authenticates, controls, monitors, and audits Unclassified users’ accesses to the remote Classified network, while providing each connected network with a very high degree of protection against unauthorized access and penetration attempts by outsiders.

3.1.8.1 Trusted Portal Server

The Trusted Portal Server application enforces strict separation of the connected networks while performing the access control and session mediation functions that allow positively authenticated, authorized Dual-Mode Secure Workstation users working on an Unclassified network to access resources on a remote Classified network. The Dual-Mode Secure Workstation and the Trusted Portal mutually establish a trusted path—in practical terms, a Virtual Private Network—between themselves via a Type 1-encrypted IP Security (IPSEC) connection tunneled through the Unclassified network. This Virtual Private Network (VPN) enables the authorized Dual-Mode Secure Workstation user to access the desired Classified resources.

3.1.8.2 Dual-Mode Secure Workstation

The Dual-Mode Secure Workstation is an Intel-based PC enhanced with a set of NSA-approved COTS security components. The functions of these security components complement each other, enabling the Dual-Mode Secure Workstation to assume either of two different, absolutely isolated security roles. When it is started up, the Dual-Mode Secure Workstation defaults to Unclassified mode, booting from the Unclassified partition of the hard disk. When booted, the

system presents the user with the PC's Unclassified operating environment (e.g., Microsoft NT client) and the suite of software applications the user needs to work with Unclassified information, and to access resources on the Unclassified network to which the workstation is physically connected.

To switch to Classified mode to access the remote Classified environment, the user simply clicks on an icon on the PC screen. The Dual-Mode Secure Workstation immediately reboots itself from the encryption-protected Classified partition of the PC's hard disk, and then activates the Type 1 encrypted network interface required for the Classified session. In Classified mode, the workstation runs a completely separate operating environment and suite of application software appropriate to the tasks to be performed in Classified mode.

3.1.8.3 Security and Functionality

The Trusted Portal achieves its secure interconnection of Classified and Unclassified network/computing resources in strict accordance with DoD mandatory security policies.

Moreover, the NSA B3-evaluated XTS-300™ includes high assurance security and integrity controls sufficient to isolate and protect the Trusted Portal Server application. This allows the Trusted Portal Server to run on the same physical XTS-300™ as one of DigitalNet's high-assurance Guard applications, such as the DII Guard or the DataSync Guard, creating a flexible, multifunctional trusted gateway.

For example, by co-hosting the DII Guard with the Trusted Portal Server, the DII Guard's capabilities—which allow authorized users on the Classified network to exchange Unclassified e-mail with authorized users on the Unclassified network—are augmented by the Trusted Portal's capabilities—which allow authorized, cleared Dual-Mode Secure Workstation users on the Unclassified network to assume their "Classified" role and access the Classified messaging infrastructure to exchange Classified e-mails with other users on the Classified network.

Financial analyses show that the DigitalNet Trusted Portal can provide significant per-desktop savings in terms of initial equipment purchase, and ongoing operations, maintenance, administration, and management costs when compared with the costs associated with purchasing and operating multiple workstations and separate Classified and Unclassified network connections to each desktop.

3.2 TEMPEST/Zone

The TEMPEST Program was established to address the threat to national security posed by compromising emanations. Since the 1980's, Government agencies, particularly in the intelligence arena, have been well aware of the risks associated with the use of commercial computers and peripherals for processing sensitive and classified information. As a result, standards for the reduction/suppression of signal emissions were established for information processing equipment. The program and resulting secure equipment is referred to as TEMPEST, a code name that was once a classified term for this type of equipment. Although the name is no longer classified, the methods used to make information processing equipment secure by reducing or eliminating the equipment's electronic emissions are classified. TEMPEST is defined as the study of compromising emanations. Compromising emanations are those signals

generated by electronic equipment that, if recovered and analyzed, would divulge the information being processed by the equipment.

The requirements for TEMPEST equipment are detailed in the NSA's NSTISSAM TEMPEST/1/92 Level 1 standard. This TEMPEST standard also includes specifications for Zone-level emissions, the difference between TEMPEST and Zone being in the allowable levels/distances for electronic emissions, the TEMPEST specifications being the most stringent. Whether TEMPEST or Zone-level equipment is deployed in a particular area depends upon the organization's "Zone of Control," i.e., the extent to which the organization has control of the area in which the equipment is to be located. TEMPEST equipment is required in locations where the Zone of Control is limited or non-existent. Zone-level equipment is typically deployed at locations where there is a wide Zone of Control.

DigitalNet is a National Security Agency-endorsed TEMPEST test services facility.

DigitalNet has been one of the largest and most influential members of the U.S. TEMPEST community for more than two decades. DigitalNet is a NSA-endorsed TEMPEST Test Services Facility and Product Manufacturer under the Endorsed TEMPEST Products Program. DigitalNet employs more Certified TEMPEST Engineers than any other TEMPEST company (currently six in the United States) and supplies the world with the lion's share of secure TEMPEST and Zone products, our primary customer being the U.S. Government. DigitalNet has expertise in all aspects of TEMPEST and Zone technology – in particular, in TEMPEST and Zone systems evaluation, design, development, implementation, and maintenance.

Leveraging more than 20 years of experience in the TEMPEST/Zone arena, DigitalNet offers a full range of TEMPEST and Zone products that are tested, proven, and deliver the highest security ratings. DigitalNet TEMPEST and Zone products include servers, desktops, laptops, small form factor computers and mobile workstations, digital copiers, printers, scanners, storage devices, switches, routers, secure fax, and secure video conferencing.

TEMPEST equipment provides the most protection. However, it is more expensive than Zone equipment due to the costs associated with the development of the systems and the extensive testing the equipment must undergo to certify its TEMPEST integrity. Zone equipment is less costly, and is appropriate for a wide range of locations, such as those in which the Entry/Exit system would be in use. Zone equipment is available at a cost of about thirty percent more than commercial equipment.

Product development and testing is performed in DigitalNet's NSA-endorsed TEMPEST test services facility by NSA-certified TEMPEST Test Engineers. Of the 15,000 sq. ft. area restricted (card access) facility allocated to its secure systems organization, one-third of the space is dedicated to systems testing. Eight NSA-endorsed TEMPEST test chambers complete with endorsed test equipment support all aspects of TEMPEST/Zone testing. DigitalNet ensures TEMPEST integrity through continuous audits performed by NSA-certified TEMPEST engineers. DigitalNet's TEMPEST and Zone equipment is guaranteed to meet or surpass the requirements of the U.S. Government NSTISSAM TEMPEST/1-92 Level 1 specification, when maintained by DigitalNet TEMPEST-certified Customer Engineers.

DigitalNet has a highly trained and dedicated TEMPEST engineering staff. DigitalNet's 25-member TEMPEST R&D engineering staff, with a combined total of approximately 450 years of experience in secure systems engineering, has an in-depth understanding of TEMPEST and Zone requirements. Working in DigitalNet's comprehensive NSA-endorsed test and manufacturing facilities, they derive substantial benefits from DigitalNet's many corporate alliances and partnerships during the product development process. Their mission is to produce secure versions of the latest in information technology products as close as possible to the introduction of those products into the commercial marketplace. Upon customer request, they also work on specialized projects to customize systems to meet a customer's unique requirements, such as secure video conferencing.

DigitalNet is a full-service ISO 9002 manufacturing facility. DigitalNet's Manufacturing is a full-service ISO 9002 NSA-endorsed TEMPEST facility capable of warehousing, building, shipping, cataloging, and performing quality inspections on all aspects of the manufacturing process. ISO 9002 certification means that DigitalNet meets and has been certified by the International Standards Organization (ISO) in relation to all aspects of DigitalNet's manufacturing, logistics, and repair operations.

3.2.1 TEMPEST/Zone Options for the DHS Environment

The options for addressing the risks posed by electronic emissions in the DHS environment can be divided into four scenarios:

- The first option is to enclose the entire building with a protective shield that prevents emissions from being radiated to the outside, enabling individuals to use standard commercial equipment without risk of emissions compromise. Several facilities of this type exist, some of which were older buildings that were retrofitted and others that were built from ground up. Within such facilities, if there is a concern for the physical security of the servers, the servers are placed in GSA-approved Class V safes, to prevent unauthorized physical access to the systems. Due to the high cost of such a solution, most organizations have moved away from a consideration of this total building approach and elect one of the remaining three options.
- The second option, for a non-shielded building, is to place commercial processing equipment in a Secure Compartmented Information Facility (SCIF) – a shielded room that is constructed in much the same way as a TEMPEST test chamber within a facility. Data can be processed in a SCIF without risk of emissions beyond the walls of the SCIF. Individuals are admitted into the SCIF following highly controlled procedures.
- The third option, again in a non-shielded environment, is to place TEMPEST/Zone processing equipment in a rack-mount Class V safe, to ensure both emanations security and physical security. Special products that are available to facilitate the administration of this solution include a Fiber Reach product that, in combination with a TEMPEST or Zone monitor, keyboard and mouse, allows for administration of systems in a rack-mount configuration from an extended distance from the safe via a fiber optic link. A fiber optic link is the cable of choice in a secure environment because fiber is much harder to penetrate than standard twisted pair (CAT 5).
- The fourth solution is to put TEMPEST/Zone equipment into a facility that has adequate

physical security but no emanation security. This could include facilities that operate 24x7.

Options three and four tend to be the most cost-effective because you can pay only for the security you need.

Section 4 — DigitalNet’s Related Experience

Leveraging 30 years of experience, DigitalNet, is a leading provider of Information and Communications Technology (ICT) solutions to the U.S. Federal DigitalNet is dedicated to delivering high- and medium-assurance server, Guard, and gateway solutions for multilevel secure/multi-compartment exchange of information. DigitalNet’s solutions are based on state-of-the-art trusted computer, network, and cryptographic technologies. DigitalNet maintains a highly skilled staff of Information Assurance engineers working in dedicated security laboratory, testbed, integration, and manufacturing facilities. DigitalNet has been instrumental in implementing and deploying trusted applications in U.S. and foreign government military/defense, intelligence, diplomatic, and law enforcement installations worldwide, and in supporting the certification and accreditation of these applications. We are also the world’s top supplier of TEMPEST and Zone products that protect networks with highly sensitive information from electronic eavesdropping. Headquartered in Herndon, VA, DigitalNet has more than 2,000 employees worldwide, with more than 800 cleared for classified work.

With many years of leadership in networks and information assurance, we can maximize your network performance with an integrated, unbiased approach to high performance secure internetworking. Our portfolio offers a full range of networking and information solutions that create a computing environment right sized for your unique needs and protected against the threats that have become a daily concern. We ensure efficiency by employing tools and services that assess, measure, and optimize network performance. The following represents a subset of security centric programs DigitalNet has performed within the Federal Government.

4.1 DII and DMS Guard Program

The DigitalNet DII Guard and DMS Guard enable the automated exchange of X.400 and SMTP messages and X.500 directory information among Classified and Unclassified enclaves and networks according to site-defined release and admittance policies enforced by the Guard’s security policy filters. Developed for the NSA, the DII and DMS Guards are based on DigitalNet’s Secure Automated Guard Environment (SAGE), a Guard-specific transaction processing environment and software development framework designed to minimize the cost, time, and effort required to implement and accredit trusted guards. The Guard includes security policy filters that validate: allowable sender and recipient addresses and permissions; correct use of FORTEZZA[®], ACP 120, and MSP 3.0; transmission characteristics and content, including message classifications, message body and attachment types, X.500 operation types and authentication and dirty word scans of message bodies and attachments (ASCII and RTF).

4.2 DISA Command and Control Guard System

The DISA standard Command and Control Guard (C²G) is a two-way file transfer “store-and-forward” Guard system developed for automating command center operations as part of the DoD MLS Program (an earlier version was called the WWMCCS Guard). The C²G supports high-to-low and low-to-high data flow with fully automated review of the vast majority of the data that it processes. It is a high-assurance, standards-compliant, COTS-based Guard that currently handles text and structured data only.

C²G security policy filters are context table-driven so that they can be easily edited to handle different file types and security policies. The C²G can be configured to support different “reviewer-of-error-file” (REF) roles, so files rejected by the Guard can be queued for manual review and editing by authorized personnel, then resubmitted to the Guard. The C²G is the Guard of choice for automatically exchanging data between the Global Command and Control System (GCCS) and CinC command and control or intelligence systems.

4.3 DataSync Guard System

DigitalNet’s DataSync Guard is designed to minimize Trusted Guard impact on data transfer latencies. The DataSync Guard allows two databases’ replication processes to communicate directly with each other as they were designed to do: via TCP/IP socket connections that are mediated by the Guard. Operating transparently to the databases, the DataSync Guard strictly enforces security policy rules governing data release on every data packet flowing between the databases. It does all its processing in memory, which adds very little overhead - and time - to each data replication. The result is near-real-time replications between databases at different classification levels that keep the databases in sync within seconds of each other.

By doing most of its processing in memory, the DataSync Guard performs very few disk accesses. This is the key to its speed. And because the Guard communicates via sockets, it is protocol-independent. It can mediate all sorts of connection-oriented interprocess communications that use sockets as their transport mechanism. For organizations that store image files, large documents, or slide presentations in their databases, the DataSync Guard can be configured to simultaneously support both high-speed data replications and “out of band” file transfer. This dual-transfer-mode capability allows the DataSync Guard to keep the databases synchronized and unaffected by the higher overhead required to process the large data files.

The DataSync Guard can implement complex security policy filters to enforce releasability standards, including authorizations of originator and recipients, data header transaction checks and policy-defined checks on the content of each data element. These security policy filters are stored in the form of “filter templates” and different templates can be enforced for different originator/recipient combinations, for different data types, etc. The DataSync Guard is currently being used on a number of DoD programs.

4.4 FBI “Cyclone” Network Guard Program

DigitalNet developed an XTS-300-based trusted network guard/gateway application to enable the FBI to connect its IBM network to that of the U.S. Customs Service, to interchange data between the two agencies. DigitalNet remains under contract to the FBI, supporting the certification and accreditation, operational deployment, and functional and performance enhancements of the Guard. In addition to its original FBI-Customs deployment, the Guard is being deployed more widely to monitor and control interfaces between FBI systems and those of other national and state Government and law enforcement agencies.

4.5 Department of State Telegram Distribution Guard Program

Within the Department of State (DOS), the primary mechanism for global command and control communications is the *telegram*, which is transferred via a classified communications network

operated by the Diplomatic Telecommunications Service. The telegram is the primary document for recording DOS actions, and provides historical records through which current events can be analyzed. The ability to receive and review incoming telegram data expeditiously is essential to the DOS' mission.

The DOS needs to link its Classified and Unclassified computer networks to exchange Unclassified telegrams between the two. DigitalNet was contracted by DOS to implement an XTS-300 and SAGE-based Guard to mediate the two-way flow of telegrams between DOS Classified and Unclassified networks. The DOS Guard automatically reclassifies to Unclassified those files that meet DOS criteria for release. Downgraded files are released to the appropriate Unclassified network, while files that fail to meet DOS release criteria, or that require manual intervention, are queued for operator review using the SAGE Man-in-the-Middle interface.

Guard security policy is enforced by a set of control tables that govern parsing and review of DOS telegram content. The Guard compares each telegram against these control tables to check for presence of disallowed ASCII characters, context-sensitive text strings, words likely to indicate classified content (e.g., *Secret*), and words on a frequently changing list of sensitive situation- or event-specific text strings. The Guard includes a graphical user interface (GUI)-based editor for easy addition, deletion, and modification of control table entries.

Section 5 — Recommendations

Our recommendation to DHS to include NSA-certified High Assurance Guards and TEMPEST/Zone technology in the DHS network is based upon 22 years of experience protecting critical data for the Intelligence Community. The DHS, in our opinion, will have many of the challenges the Intelligence Community has faced for years in protecting and securing data.

5.1 Guard Technology

The Community has known for years that it must have a commitment to share information with other organizations to be effective in their mission. However, they also know that database information on certain servers should not be completely shared due to possible leaks of “sources and methods” of how that information was obtained. That level of commitment, of protecting data, must now be employed by the DHS due to the nature of the mission and the multiple agencies that will now have to share data. Those agencies are running at different levels of security classification and in some cases their classification sources are different. For example, the Justice Department and the Treasury Department have different methodologies for providing security clearances for employees and contractors.

The agencies that are participating in DHS will want to protect their own internal directories because that is where all the critical information about an organization is stored. As databases located on different systems begin to share data as never before, the owner-agency of the data will want to ensure that they are doing everything possible to succeed in the mission of the DHS but still want to protect data that has no relevance for the other agencies. Each of the agencies that will participate in the DHS will have their own unique PKI and advanced authentication methodologies and practices. However, those differences, if not managed properly, could impact the success of DHS. As employees of all the agencies begin to share information via e-mail, in a new spirit of cooperation, agency security managers will now have to be concerned about what is being released via e-mail.

The Guard technology has a place in the DHS because it has been solving these problems for the Intelligence Community for many years. The Guards protect databases, agency directories, border directories, database synchronizations, boundaries, encryption methodologies, perimeter protection, portal protection and multiple security classifications. However, before they can do any of this work in the Intelligence Community, they must be certified by NSA. All the certification work has been done and now the DHS can benefit from the years of experience and work that went into this technology. These are not products that have just come from the drawing boards and now must be tested in the “real world” as often times happens when new products are introduced. These products have the test of time on their side and certifications by a well respected security focused organization.

5.2 TEMPEST/Zone Technology

The Intelligence Community has also learned from years of experience how electronic emanations can compromise security and their mission. Networks can be built with the latest and

most sophisticated fire walls, intrusion detection systems, advanced authentication technology, encryption and other technologies designed to protect data as it is moving through a network.

However, that network can be compromised very easily by people using inexpensive electronic devices “peeking” at data on display terminals and output from printers, scanners, digital copiers, etc. COTS technology “broadcasts” what they are working on. Electronic emanations are part and parcel of this technology. However, in some cases users cannot afford to have their COTS products telling the world what they are working on. This is where TEMPEST/Zone technology will become important to the DHS. Where DHS users cannot guarantee that no one is eavesdropping on their work being done on COTS devices.

In most cases, COTS products will be more than capable of performing the mission of the DHS without concern. However, in those cases the DHS managers will have complete control over the physical environment of the offices used to produce or retrieve the data. However, in those cases where the DHS user is not in complete control of the physical environment, TEMPEST/Zone technology will have a place in the DHS.

In addition to all the TEMPEST and Zone technology that we have produced, we know that there may be unknown unique electronic emanation elimination/suppression requirements that will arise because of DHS. During our 22-year history of manufacturing TEMPEST technology for the Intelligence Community, we have become very adept at “TEMPEST-izing” newer technology as it is being introduced to the main stream.

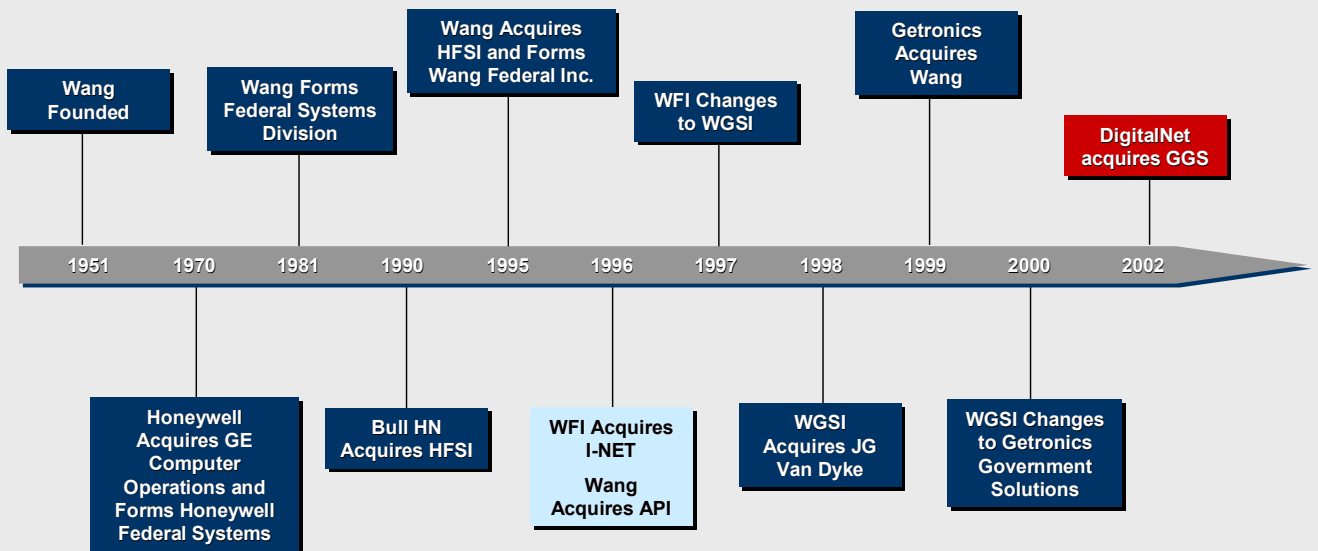
As an example of that commitment, the Intelligence Community recently realized that digital copiers pose a significant threat due to the way they emanate. And since analog copiers are being phased out by most manufacturers, the Community came to us with their problem. We quickly “TEMPEST-ized” a digital copier of their choice and had it certified by NSA. Now the networked or stand-alone digital copiers will not compromise their mission. If the DHS is faced with a challenge to “TEMPEST-ize” a product, we can do it for you.

We appreciate the reader spending the time to learn more about the potential information assurance solutions for the Department of Homeland Security and the agencies that comprise this new Department. We would encourage the Government to include some performance or functional requirements in the DHS network to address the mitigation of the four risks we have identified in this white paper which are; ***directory interfacing and data sharing, sharing of releasable data, cryptographic interoperability and electronic emissions.***

In many cases within the civilian government agencies security has been an issue that has been considered something that constrains the mission of the agency. However, these technologies addressed in this paper, are “enabling” technologies because the agency mission, in many cases, could not be accomplished without them.

We hope that some of the information contained in this document has proven useful in the development of the Department of Homeland Security network.

The Road to DigitalNet



DIGITALNET PROPRIETARY INFORMATION

The graph above describes the history of acquisitions that created DigitalNet