United States Government Accountability Office

GAO

Report to Congressional Requesters

June 2008

INFORMATION SECURITY

Federal Agency Efforts to Encrypt Sensitive Information Are Under Way, but Work Remains

GAO

Accountability ★ Integrity ★ Reliability

GAO
Accountability·Integrity·Reliability
Highlights

Highlights of GAO-08-525, a report to congressional requesters

June 2008

INFORMATION SECURITY

Federal Agency Efforts to Encrypt Sensitive Information Are Under Way, but Work Remains

Why GAO Did This Study

Many federal operations are supported by automated systems that may contain sensitive information such as national security information that, if lost or stolen, could be disclosed for improper purposes. Compromises of sensitive information at numerous federal agencies have raised concerns about the extent to which such information is vulnerable. The use of technological controls such as encryption—the process of changing plaintext into ciphertext—can help guard against the unauthorized disclosure of sensitive information.

GAO was asked to determine (1) how commercially available encryption technologies can help agencies protect sensitive information and reduce risks; (2) the federal laws, policies, and guidance for using encryption technologies; and (3) the extent to which agencies have implemented, or plan to implement, encryption technologies. To address these objectives, GAO identified and evaluated commercially available encryption technologies, reviewed relevant laws and guidance, and surveyed 24 major federal agencies.

What GAO Recommends

GAO is making recommendations to (1) the Director of the Office of Management and Budget (OMB) to clarify guidance and (2) selected agencies to strengthen practices for planning and implementing the use of encryption. In comments on a draft of this report, OMB and the agencies generally agreed with the recommendations.

To view the full product, including the scope and methodology, click on GAO-08-525. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

Commercially available encryption technologies can help federal agencies protect sensitive information that is stored on mobile computers and devices (such as laptop computers, handheld devices such as personal digital assistants, and portable media such as flash drives and CD-ROMs) as well as information that is transmitted over wired or wireless networks by reducing the risks of its unauthorized disclosure and modification. For example, information stored in individual files, folders, or entire hard drives can be encrypted. Encryption technologies can also be used to establish secure communication paths for protecting data transmitted over networks. While many products to encrypt data exist, implementing them incorrectly—such as failing to properly configure the product, secure encryption keys, or train users—can result in a false sense of security and render data permanently inaccessible.

Key laws frame practices for information protection, while federal policies and guidance address the use of encryption. The Federal Information Security Management Act of 2002 mandates that agencies implement information security programs to protect agency information and systems. In addition, other laws provide guidance and direction for protecting specific types of information, including agency-specific information. For example, the Privacy Act of 1974 requires that agencies adequately protect personal information, and the Health Insurance Portability and Accountability Act of 1996 requires additional protections for sensitive health care information. The Office of Management and Budget has issued policy requiring federal agencies to encrypt all data on mobile computers and devices that carry agency data and use products that have been approved by the National Institute for Standards and Technology (NIST) cryptographic validation program. Further, NIST guidance recommends that agencies adequately plan for the selection, installation, configuration, and management of encryption technologies.

The extent to which 24 major federal agencies reported that they have implemented encryption and developed plans to implement encryption of sensitive information varied across agencies. From July through September 2007, the major agencies collectively reported that they had not yet installed encryption technology to protect sensitive information on about 70 percent of their laptop computers and handheld devices. Additionally, agencies reported uncertainty regarding the applicability of OMB's encryption requirements for mobile devices, specifically portable media. While all agencies have initiated efforts to deploy encryption technologies, none had documented comprehensive plans to guide encryption implementation activities such as installing and configuring appropriate technologies in accordance with federal guidelines, developing and documenting policies and procedures for managing encryption technologies, and training users. As a result federal information may remain at increased risk of unauthorized disclosure, loss, and modification.

Contents

Tables

Figures

Abbreviations

CD-ROM	compact disc read only memory
DVD	digital versatile disc
FIPS	federal information processing standards
FISMA	Federal Information Security Management Act of 2002
GSA	General Services Administration
HUD	Department of Housing and Urban Development
IT	information technology
NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PKI	public key infrastructures
SmartBUY	Software Managed and Acquired on the Right Terms
USB	universal serial bus
US-CERT	U.S. Computer Emergency Readiness Team
USDA	U.S. Department of Agriculture

G A O

Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

June 27, 2008

The Honorable Bennie G. Thompson
Chairman
Committee on Homeland Security
House of Representatives

The Honorable Jane Harman
Chairwoman
Subcommittee on Intelligence, Information
Sharing and Terrorism Risk Assessment
Committee on Homeland Security
House of Representatives

The Honorable Zoe Lofgren
House of Representatives

In 2006, the Department of Veterans Affairs reported that a laptop computer and external hard drive—that had not been encrypted or password protected and that contained the personal information of approximately 26.5 million veterans and United States military personnel—had been stolen from an employee's home. This incident and the increasing number of data breaches reported by other government agencies—such as the Departments of Defense and Health and Human Services and the Transportation Security Administration—have raised concerns about the extent to which sensitive information maintained by the federal government is vulnerable and what current laws, policies, and practices are in place to protect that information.[1]

In June 2006, GAO testified that federal agencies should consider the use of encryption technologies to improve their ability to protect information

[1] As used in this report, the term "sensitive information" refers to any information that an agency has determined requires some degree of heightened protection from unauthorized access, use, disclosure, disruption, modification, or destruction because of the nature of the information, e.g., personal information required to be protected by the Privacy Act of 1974, proprietary commercial information, information critical to agency program activities, and information that has or may be determined to be exempt from public release under the Freedom of Information Act.

from improper disclosure,[2] particularly when data must be stored on mobile computers and devices such as laptop computers, handheld personal digital assistants, and portable media such as flash drives and CD-ROMs. Encryption protects data through a process of transforming ordinary data (commonly referred to as plaintext) into code form (ciphertext) using a special value known as a key and a mathematical process called an algorithm. [3] Encryption technologies include commercially available products (such as hardware or software) that create the capability to encrypt data.

In response to your request, our objectives were to determine (1) how commercially available encryption technologies could help federal agencies protect sensitive information and reduce risks; (2) the federal laws, policies, and guidance for using encryption technologies to protect sensitive information; and (3) the extent to which agencies have implemented, or planned to implement, encryption technologies to protect sensitive information.

To address these objectives, we identified commercially available encryption technologies by reviewing prior GAO reports on technology, researching products approved by the National Institute of Standards and Technology (NIST), and interviewing NIST encryption experts. We also reviewed relevant laws, policies, and guidance to identify the mandatory and optional practices for protecting sensitive information (including personally identifiable information[4]) that federal agencies collect and handle. In addition, we surveyed 24 major federal agencies and examined supporting documentation regarding agency efforts to implement

[2] GAO, *Privacy: Preventing and Responding to Improper Disclosures of Personal Information*, GAO-06-833T(Washington, D.C.: June 8, 2006).

[3] Encryption is a subset of cryptography, which is used to secure transactions by providing ways to ensure data confidentiality (assurance that the information will be protected from unauthorized access), data integrity (assurance that data have not been accidentally or deliberately altered), authentication of the message's originator, electronic certification of data, and nonrepudiation (proof of the integrity and origin of data that can be verified by a third party).

[4] For purposes of this report, the terms "personally identifiable information" and "personal information" refer to any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, or biometric records, and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

encryption.[5] We also examined encryption practices at six of these agencies to determine whether these practices met federal requirements for installation and configuration of Federal Information Processing Standards (FIPS)-validated cryptographic modules, encryption products, and associated management controls.

We conducted this performance audit from February 2007 through June 2008 in accordance with generally accepted government auditing standards. These standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Appendix I contains additional details on the objectives, scope, and methodology of our review.

Results in Brief

Many types of commercially available encryption technologies can help federal agencies protect sensitive information and reduce the risks to the sensitive data stored on agency equipment or transmitted across a network. Data stored in individual files, folders, or entire drives can be encrypted when not in use. Types of technologies to protect stored data include full disk encryption, hardware-based encryption, and file, folder, or virtual disk encryption. In addition, encryption technologies can be used to establish secure communication paths for protecting data transmitted over networks through the use of virtual private networks and digital certificates. While many technologies to encrypt data exist, implementing them incorrectly—such as failing to properly configure the product, secure encryption keys, or train users—can create a false sense of security and even render data permanently inaccessible.

Although key federal laws do not specifically address the use of encryption, they provide a framework of information protection activities and direct the Office of Management and Budget (OMB) and NIST to develop policies, standards, and guidance for federal agencies to use in implementing technologies, such as encryption, to protect sensitive

[5] The 24 major federal agencies are the Agency for International Development; the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency; the General Services Administration; the National Aeronautics and Space Administration; the National Science Foundation; the Nuclear Regulatory Commission; the Office of Personnel Management; the Small Business Administration; and the Social Security Administration.

information. Among these laws is the Federal Information Security Management Act of 2002 (FISMA), which mandates that agencies implement information security programs to protect agency information and systems. In addition, the Privacy Act of 1974 requires that agencies adequately protect personal information maintained in federal systems of records,[6] and the Health Insurance Portability and Accountability Act of 1996 addresses the protection of personal medical information. To specifically direct agencies' use of encryption, OMB issued a policy in 2006 recommending, and in 2007 requiring, that all agencies encrypt all data on mobile computers and devices that carry sensitive agency data and also reinforced the long-standing requirement that agencies use products that have been approved by NIST's cryptographic module validation program. Further, NIST has published guidelines for federal agencies to use in planning and implementing encryption technologies; these guidelines address the documentation of comprehensive implementation plans; the installation and configuration of selected encryption technologies, policies and procedures for managing encryption; and user training.

The extent to which 24 major federal agencies reported that they have implemented encryption and to which they have developed plans to implement encryption varied across the agencies. While all agencies had initiated efforts to encrypt sensitive agency information, the encryption of information stored on mobile devices lagged behind efforts to encrypt information transmitted over networks. For example, overall, agencies reported in July through September 2007 that they had not yet installed encryption software on about 70 percent of their laptop computers and handheld mobile computing devices combined. Although progress was under way at agencies governmentwide, agencies reported uncertainty regarding the applicability of OMB's encryption requirements. In addition, none of the agencies had documented comprehensive plans to guide encryption implementation activities, such as inventorying information to determine encryption needs; documenting how the agency plans to select, install, configure, and monitor encryption technologies; developing and documenting encryption policies and procedures; and training personnel in the use of installed encryption. Further, our tests at 6 selected agencies revealed weaknesses in the encryption implementation practices involving the installation and configuration of FIPS-validated cryptographic modules, encryption products, monitoring the effectiveness of installed

[6] "System of records" is defined as a group of records under the control of an agency from which information is retrieved by the name of the individual or by an individual identifier.

encryption technologies, the development and documentation of policies and procedures for managing these technologies, and training of personnel in the proper use of installed encryption products. As a result of these weaknesses, federal information may remain at increased risk of unauthorized disclosure, loss, and modification.

We are recommending that OMB clarify governmentwide encryption policy to address agency efforts to plan for and implement encryption technologies. We are also making recommendations to selected agencies to properly install and configure FIPS-compliant encryption technologies, to develop policies and procedures to manage encryption, and to provide encryption training to personnel.

We obtained written comments on a draft of this report from OMB, the Departments of Education, Housing and Urban Development, and State, as well as the General Services Administration and the National Aeronautics and Space Administration; these comments are reproduced in appendixes V to X, respectively. We also obtained comments from the Department of Agriculture via e-mail. OMB generally agreed with the report's contents and stated that it would carefully consider our recommendations. The other six agencies also agreed with the report's findings and recommendations. In addition, NIST and the Social Security Administration provided technical comments, which we have incorporated as appropriate.

Background

Virtually all federal operations are supported by automated systems, mobile devices, and electronic media that may contain sensitive information such as Social Security numbers, medical records, law enforcement data, national or homeland security information, and proprietary information that could be inappropriately disclosed, browsed, or copied for improper or criminal purposes.

In our survey of 24 major federal agencies, 10 agencies reported having systems that contain sensitive medical information, 16 reported having systems that contain sensitive regulatory information, 19 reported having systems that contain sensitive personal information, and 20 reported having systems that contain sensitive program-specific information. It is important for agencies to safeguard sensitive information because, if left unprotected, the information could be compromised—leading to loss or theft of resources (such as federal payments and collections), modification or destruction of data, or unauthorized use of computer resources, including launching attacks on other computer systems.

Factors Placing Sensitive Information at Risk

Many factors can threaten the confidentiality, integrity, and availability of sensitive information. Cyber threats to federal systems and critical infrastructures containing sensitive information can be intentional or unintentional, targeted or nontargeted, and can come from a variety of sources.[7] Intentional threats include both targeted and nontargeted attacks. A targeted attack occurs when a group or individual specifically attacks an information system. A nontargeted attack occurs when the intended target of the attack is uncertain, such as when a virus, worm, or malware is released on the Internet with no specific target. Unintentional threats can be caused by software upgrades or maintenance procedures that inadvertently disrupt systems.

The Federal Bureau of Investigation has identified multiple sources of threats to our nation's critical information systems, including those from foreign nation states engaged in information warfare, domestic criminals, hackers, virus writers, and disgruntled current and former employees working within an organization. There is increasing concern among both government officials and industry experts regarding the potential for a cyber attack. According to the Director of National Intelligence, "our information infrastructure—including the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries—increasingly is being targeted for exploitation and potentially for disruption or destruction by a growing array of state and non-state adversaries. Over the past year, cyber exploitation activity has grown more sophisticated, more targeted, and more serious. The intelligence community expects these trends to continue in the coming year."[8]

Threats to mobile devices are posed by people with malicious intentions, including causing mischief and disruption as well as committing identity theft and other forms of fraud. For example, malware threats can infect data stored on devices, and data in transit can be intercepted through many means, including from e-mail, Web sites, file downloads, file sharing, peer-to-peer software, and instant messaging. Another threat to mobile devices is the loss or theft of the device. Someone who has physical access to an electronic device can attempt to view the information stored on it.

[7] Critical infrastructures include cyber and physical, public and private infrastructures that are essential to national security, national economic security, or national public health and safety.

[8] J. Michael McConnell, *Annual Threat Assessment of the Director of National Intelligence for the Senate Select Committee on Intelligence*, Feb. 5, 2008.

Incidents at Federal Agencies Demonstrate That Sensitive Information Is at Risk

Examples of Data Breaches at Federal Agencies

Defense
February 2008
A laptop computer containing personally identifiable information for as many as 4,000 participants in the Marine Corps community services' New Parent Support Program was stolen.

Energy
December 2007
A hacker gained access to an Energy computer by embedding a program, in an e-mail sent to staff, that allowed the hacker to copy and retrieve information.

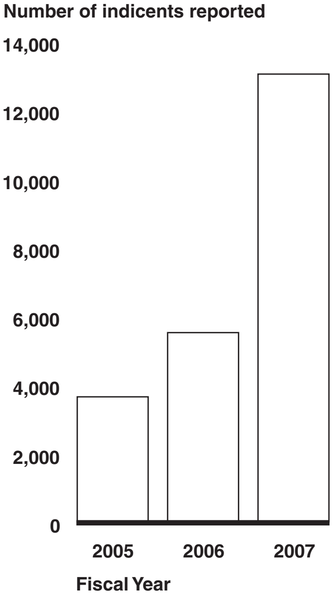
Transportation Security Administration
May 2007
An external hard drive, discovered missing from a controlled area at agency headquarters human capital office, contained personal data for 100,000 archived employment records of individuals employed by the agency from January 2002 until August 2005.

Source: GAO based on agency-reported incidents.

The need for effective information security policies and practices is further illustrated by the increasing number of security incidents reported by federal agencies that put sensitive information at risk. Personally identifiable information about millions of Americans has been lost, stolen, or improperly disclosed, thereby potentially exposing those individuals to loss of privacy, identity theft, and financial crimes. Reported attacks and unintentional incidents involving critical infrastructure systems demonstrate that a serious attack could be devastating. Agencies have experienced a wide range of incidents involving data loss or theft, computer intrusions, and privacy breaches, underscoring the need for improved security practices.

When incidents occur, agencies are to notify the federal information security incident center—the U.S. Computer Emergency Readiness Team (US-CERT). As shown in figure 1, the number of incidents reported by federal agencies to US-CERT has increased dramatically over the past 3 years, increasing from 3,634 incidents reported in fiscal year 2005 to 13,029 incidents in fiscal year 2007 (about a 259 percent increase).

Figure 1: Incidents Reported to US-CERT in Fiscal Years 2005 through 2007



Source: GAO analysis of US-CERT data.

Data breaches present federal agencies with potentially serious and expensive consequences; for example, a security breach might require an agency to fund the burdensome costs of notifying affected individuals and associated credit monitoring services or it could jeopardize the agency's mission. Implementation of a risk-based framework of management, operational, and technical controls that includes controls such as encryption technology can help guard against the inadvertent compromise of sensitive information. While encrypting data might add to operational burdens by requiring individuals to enter pass codes or use other means to encrypt and decrypt data, it can also help to mitigate the risk associated with the theft or loss of computer equipment that contains sensitive data.

Workforce Mobility Introduces Additional Risks to Sensitive Information

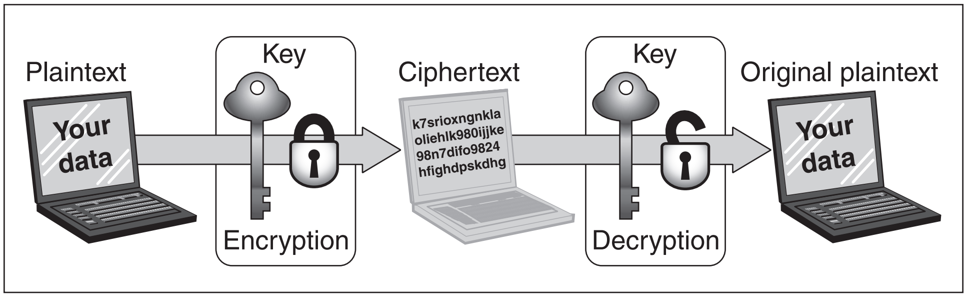
Protecting information has become more challenging in today's IT environment of highly mobile workers and decreasing device size. Using small, easily pilferable devices such as laptop computers, handheld personal digital assistants, thumb-sized Universal Serial Bus (USB) flash drives, and portable electronic media such as CD-ROMs and DVDs, employees can access their agency's systems and information from anywhere. When computers were larger and stationary, sensitive information that was stored on mainframe computers was accessible by only a limited number of authorized personnel via terminals that were secured within the physical boundaries of the agency's facility. Now, mobile workers can process, transport, and transmit sensitive information anywhere they work. This transition from a stationary environment to a mobile one has changed the type of controls needed to protect the information.[9] Encryption technologies, among other controls, provide agencies with an alternate method of protecting sensitive information that compensates for the protections offered by the physical security controls of an agency facility when the information is removed from, or accessed from, outside of the agency location.

Encryption Can Help Protect Sensitive Information

Data breaches can be reduced through the use of encryption, which is the process of transforming plaintext into ciphertext using a special value known as a key and a mathematical process called an algorithm (see fig. 2).

[9] Security controls—access controls—should provide reasonable assurance that computer resources (data files, application programs, and computer-related facilities and equipment) are protected. Such controls include physical access controls, such as keeping computers in locked rooms, and logical access controls, such as security software programs designed to prevent or detect unauthorized access to sensitive files.

Figure 2 : Encryption and Decryption



Source: GAO analysis.

Cryptographic algorithms are designed to produce ciphertext that is unintelligible to unauthorized users. Decryption of ciphertext—returning the encoded data to plaintext—is possible by using the proper key. Encryption can protect sensitive information in storage and during transmission. Encryption of data in transit hides information as it moves, for example, between a database and a computing device over the Internet, local networks, or via fax or wireless networks. Stored data include data stored in files or databases, for example, on a personal digital assistant, a laptop computer, a file server, a DVD, or a network storage appliance. Encryption may also be used in system interconnection devices such as routers, switches, firewalls, servers, and computer workstations to apply the appropriate level of encryption required for data that pass through the interconnection.[10]

Commercially Available Encryption Technologies Can Help Agencies Reduce Risks

Commercially available encryption technologies can help federal agencies protect sensitive information and reduce the risks of its unauthorized disclosure and modification. These technologies have been designed to protect information stored on computing devices or other media and transmitted over wired or wireless networks.

Because the capability of each type of encryption technology to protect information is limited by the boundaries of the file, folder, drive, or network covered by that type of technology, a combination of several technologies may be required to ensure that sensitive information is continuously protected as it flows from one point, such as a remote mobile device, to another point, such as a network or portable electronic media.

[10] A system interconnection is the direct connection of two or more IT systems for the purpose of sharing data and other information resources.

For example, one product that encrypts a laptop's hard drive may not provide any protection for files copied to portable media, attached to an e-mail, or transmitted over a network.

Encryption Technologies to Protect Stored Information Are Available

Agencies have several options available when selecting an encryption technology for protecting stored data. According to NIST guidance on encrypting stored information,[11] these include full disk, hardware-based, file, folder, or virtual disk encryption. Through the use of these technologies, encryption can be applied granularly, to an individual file that contains sensitive information, or broadly, by encrypting an entire hard drive. The appropriate encryption technology for a particular situation depends primarily on the type of storage, the amount of information that needs to be protected, and the threats that need to be mitigated. Storage encryption technologies require users to authenticate successfully before accessing the information that has been encrypted. The combination of encryption and authentication controls access to the stored information.

Full Disk Encryption

Full disk encryption software encrypts all data on the hard drive used to boot a computer, including the computer's operating system, and permits access to the data only after successful authentication to the full disk encryption software. The majority of current full disk encryption products are implemented entirely within a software application. The software encrypts all information stored on the hard drive and installs a special environment to authenticate the user and begin decrypting the drive. Users enter their user identification and password before decrypting and starting the operating system. Once a user authenticates to the operating system by logging in, the user can access the encrypted files without further authentication, so the security of the solution is heavily dependent on the strength of the operating system authenticator.

When a computer is turned off, all the information encrypted by full disk encryption is protected, assuming that pre-boot authentication is required. After the computer is booted, full disk encryption provides no protection and the operating system becomes fully responsible for protecting the unencrypted information.

[11] NIST, Special Publication 800-11, *Guide to Storage Encryption Technologies for End User Devices* (Gaithersburg, Maryland: November 2007).

Hardware-Based Encryption

Full disk encryption can also be built into a hard drive. Hardware and software-based full disk encryption offer similar capabilities through different mechanisms. When a user tries to boot a device protected with hardware-based full disk encryption, the hard drive prompts the user to authenticate before it allows an operating system to load. The full disk encryption capability is built into the hardware in such a way that it cannot be disabled or removed from the drive. The encryption code and authenticators, such as passwords and cryptographic keys,[12] are stored securely on the hard drive. Because the encryption and decryption are performed by the hard drive itself, without any operating system participation, typically there is very little performance impact.

A major difference between software- and hardware-based full disk encryption is that software-based full disk encryption can be centrally managed, but hardware-based full disk encryption can usually be managed only locally. This makes key management and recovery actions considerably more resource-intensive and cumbersome for hardware-based full disk encryption than for software-based. Another major difference is that because hardware-based full disk encryption performs all cryptographic processing within the hard drive's hardware, it does not need to place its cryptographic keys in the computer's memory, potentially exposing the keys to malware and other threats. A third significant difference is that hardware-based full disk encryption does not cause conflicts with software that modifies the master boot record, for example, software that allows the use of more than one operating system on a hard drive.

File, Folder, and Virtual Disk Encryption

File, folder, and virtual disk encryption are all used to encrypt specified areas of data on a storage medium such as a laptop hard drive. File encryption encrypts files, a collection of information logically grouped into a single entity and referenced by a unique name, such as a file name. Folder encryption encrypts folders, a type of organizational structure used to group files. Virtual disk encryption encrypts a special type of file—called a container—that is used to encompass and protect other files.

File encryption is the process of encrypting individual files on a storage medium and permitting access to the encrypted data only after proper authentication is provided. Folder encryption is very similar to file

[12] A key is a value used to control cryptographic operations, such as decryption, encryption, signature generation, or signature verification.

encryption, except that it addresses individual folders instead of files. Some operating systems offer built-in file and/or folder encryption capabilities, and many third-party programs are also commercially available. File/folder encryption does not provide any protection for data outside the protected files or folders such as unencrypted temporary files that may contain the contents of any unencrypted files being held in computer memory.

Virtual disk encryption is the process of encrypting a container. The container appears as a single file but can hold many files and folders that are not seen until the container is decrypted. Access to the data within the container is permitted only after proper authentication is provided, at which point the container appears as a logical disk drive that may contain many files and folders. Virtual disk encryption does not provide any protection for data created outside the protected container, such as unencrypted temporary files, that could contain the contents of any unencrypted files being held in computer memory.

Agency Information Can Be Encrypted while in Transit over a Network

Sensitive data are also at risk during transmission across unsecured—untrusted—networks such as the Internet. For example, as reported by NIST,[13] transmission of e-mail containing sensitive information or direct connections for the purpose of processing information between a mobile device and an internal trusted system can expose sensitive agency data to monitoring or interception. According to both NIST[14] and an industry source,[15] agencies can use commercially available encryption technologies such as virtual private networks and digital signatures to encrypt sensitive data while they are in transit over a wired or wireless network.

Virtual Private Networks

According to NIST,[16] a virtual private network is a data network that enables two or more parties to communicate securely across a public network by creating a private connection, or "tunnel," between them.

[13] NIST, Information Technology Laboratory Bulletin: *Advising Users on Information Technology*, (Gaithersburg, Maryland: March 2007).

[14] NIST, Special Publication 800-11.

[15] Microsoft Corporation, *Windows Mobile Devices and Security: Protecting Sensitive Business Information*, (March 2006).

[16] NIST, Special Publication 800-47, *Security Guide for Interconnecting Information Technology Systems*, (Gaithersburg, Maryland: August 2002).

Because a virtual private network can be used over existing networks such as the Internet, it can facilitate the secure transfer of sensitive data across public networks. Virtual private networks can also be used to provide a secure communication mechanism for sensitive data such as Web-based electronic transactions and to provide secure remote access to an organization's resources.

Digital Signatures and Digital Certificates

Properly implemented digital signature technology uses public key cryptography to provide authentication, data integrity, and nonrepudiation for a message or transaction. As NIST states,[17] public key infrastructures[18] (PKI) can be used not only to encrypt data but also to authenticate the identity of specific users. Just as a physical signature provides assurance that a letter has been written by a specific person, a digital signature is an electronic credential created using a party's private key with an encryption algorithm. [19] When it is added to a document, it can be used to confirm the identity of a document's sender since it also contains the user's public key and name of the encryption algorithm. [20] Validating the digital signature not only confirms who signed it, but also ensures that there have been no alterations to the document since it was signed.

Digital signatures may also be employed in authentication protocols to confirm the identity of the user before establishing a session. Specifically, digital signatures can be used to provide higher assurance authentication (in comparison with passwords) when establishing virtual private networks.

Digital signatures are often used in conjunction with digital certificates. A digital certificate is an electronic credential that guarantees the

[17] NIST, Special Publication 800-25, *Federal Agency Use of Public Key Technology for Digital Signatures and Authentication*, (Gaithersburg, Maryland: October 2000).

[18] Public key infrastructure is a system of hardware, software, policies, and people that, when fully and properly implemented, can provide a suite of information security assurances—including confidentiality, data integrity, authentication, and nonrepudiation—that are important in protecting sensitive communications and transactions. For more information about public key infrastructure, see GAO, *Information Security: Advances and Remaining Challenges to Adoption of Public Key Infrastructure Technology*, GAO-01-277 (Washington, D.C.: Feb. 26, 2001).

[19] A private key is the secret part of an asymmetric key pair that is typically used to digitally sign or decrypt data.

[20] A public key is the public part of an asymmetric key pair that is typically used to verify signatures or encrypt data.

association between a public key and a specific entity, such as a person or organization. As specified by NIST, the signature on the document can be validated by using the public key from the digital certificate issued to the signer. Validating the digital certificate, the system can confirm that the user's relationship to the organization is still valid. The most common use of digital certificates is to verify that a user sending a message is who he or she claims to be and to provide the receiver with a means to encode a reply. For example, an agency virtual private network could use these certificates to authenticate the identity of the user, verify that the key is still good, and that he or she is still employed by the agency.

Encryption Technologies Available for Handheld Mobile Computing Devices

NIST guidance further states that encryption software can be used to protect the confidentiality of sensitive information stored on handheld mobile computing devices and mirrored on the desktop computer.[21] The information on the handheld's add-on backup storage modules can also be encrypted when not in use. This additional level of security can be added to provide an extra layer of defense, further protecting sensitive information stored on handheld devices.

In addition, encryption technologies can protect data on handheld devices while the data are in transit. Users often subscribe to third-party wireless Internet service providers, which use untrusted networks; therefore, the handheld device would require virtual private network software and a supporting corporate system to create a secure communications tunnel to the agency.

Table 1 describes the types of commercial encryption technologies available to agencies.

[21] NIST Special Publication 800-48, *Wireless Network Security 802.11, Bluetooth and Handheld Devices*, (Gaithersburg, Maryland: November 2002).

Table 1: Commercially Available Encryption Technologies

Technology	Use	Description
Full disk encryption (software)	Stored data	Full disk encryption software encrypts all data on the hard drive that is used first when a computer is turned on, including the computer's operating system, and permits access to the data only after successful authentication to the full disk encryption software.
Hardware-based encryption	Stored data	Full disk encryption can also be built into a hard drive.
File encryption	Stored data	File encryption is the process of encrypting individual files on a storage medium and permitting access to the encrypted data only after proper authentication is provided.
Folder encryption	Stored data	Folder encryption is very similar to file encryption, only it addresses individual folders instead of files.
Virtual disk encryption	Stored data	Virtual disk encryption is the process of encrypting a file called a container, which can hold many files and folders. Access to the data within the container is permitted only after proper authentication is provided.
Virtual private networks	Data in transit	A virtual private network serves as an encrypted tunnel to provide a secure communications mechanism for data in transit between networks.
Digital signatures and digital certificates	Stored data and data in transit	A digital signature is an electronic credential created using a party's private key with an encryption algorithm. A digital certificate is an electronic credential that guarantees the association between a public key and a specific entity.
Handheld mobile computing devices	Stored data and data in transit	Commercial encryption technologies allow users to send and receive encrypted e-mail and access data wirelessly using secure NIST-approved algorithms. Data stored on the handheld mobile computing devices (for example, e-mail messages, contacts, and appointments) can also be encrypted.

Source: GAO analysis, Defense Information Systems Agency, Vendor Technical Overview, and NIST special publications.

While many technologies exist to protect data, implementing them incorrectly—such as failing to properly configure the product, secure encryption keys, or train users—can result in a false sense of security or even render data permanently inaccessible. See appendix II for a discussion of decisions agencies face and important considerations for effectively implementing encryption to reduce agency risks.

Key Laws Frame Practices for Information Protection, while Federal Policies and Guidance Address Use of Encryption

Although federal laws do not specifically require agencies to encrypt sensitive information, they give federal agencies responsibilities for protecting it. Specifically, FISMA, included within the E-Government Act of 2002,[22] provides a comprehensive framework for ensuring the effectiveness of information security controls over federal agency information and information systems. In addition, other laws frame practices for protecting specific types of sensitive information. OMB is responsible for establishing governmentwide policies and for providing guidance to agencies on how to implement the provisions of FISMA, the Privacy Act, and other federal information security and privacy laws. In the wake of recent security breaches involving personal data, OMB issued guidance in 2006 and 2007 reiterating the requirements of these laws and guidance. In this guidance, OMB directed, among other things, that agencies encrypt data on mobile computers or devices and follow NIST security guidelines. In support of federal laws and policies, NIST provides federal agencies with planning and implementation guidance and mandatory standards for identifying and categorizing information types, and for selecting adequate controls based on risk, such as encryption, to protect sensitive information.

Key Laws Provide Framework for Protecting Sensitive Information

Although federal laws do not specifically address the use of encryption, they provide a framework for agencies to use to protect their sensitive information. FISMA, which is Title III of the E-Government Act of 2002, emphasizes the need for federal agencies to develop, document, and implement programs using a risk-based approach to provide information security for the information and information systems that support their operations and assets. Its purposes include the following:

- providing a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets;
- recognizing the highly networked nature of the current federal computing environment and providing effective governmentwide management and oversight of the related information security risks, including coordination of information security efforts throughout the civilian, national security, and law enforcement communities;

[22] Pub. L. No. 107-347 (Dec. 17, 2002).

- providing for development and maintenance of minimum controls required to protect federal information and information systems;

- acknowledging that commercially developed information security products offer advanced, dynamic, robust, and effective information security solutions, reflecting market solutions for the protection of critical information infrastructures important to the national defense and economic security of the nation that are designed, built, and operated by the private sector; and

- recognizing that the selection of specific technical hardware and software information security solutions should be left to individual agencies choosing from among commercially developed products.

This act requires agencies to provide cost-effective controls to protect federal information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction, and it directs OMB and NIST to establish policies and standards to guide agency implementation of these controls, which may include the use of encryption.

The E-Government Act of 2002 also strives to enhance protection for personal information in government information systems by requiring that agencies conduct privacy impact assessments. A privacy impact assessment is an analysis of how personal information is collected, stored, shared, and managed in a federal system.

Additionally, the Privacy Act of 1974 regulates agencies' collection, use, and dissemination of personal information maintained in systems of records. In this regard, the Privacy Act requires agencies to establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records and to protect against any threats or hazards to their security or integrity that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.

Congress has also passed laws requiring protection of sensitive information that are agency-specific or that target a specific type of information. These laws include the Health Insurance Portability and Accountability Act of 1996,[23] which requires additional protections to

[23] Pub. L. No. 104-191 (Aug. 21, 1996).

sensitive health care information and the Veterans Benefits, Health Care, and Information Technology Act,[24] enacted in December 2006, which establishes information technology security requirements for personally identifiable information that apply specifically to the Department of Veterans Affairs.

Table 2 summarizes the laws that provide a framework for agencies to use in protecting sensitive information.

Table 2: Key Laws That Provide a Framework for Agencies to Use in Protecting Sensitive Information

Law	Security elements
Federal Information Security Management Act of 2002	Governs information security in the federal government. Defines roles and responsibilities for OMB and NIST in developing federal policies and guidance. Also addresses the protection of sensitive information in the context of securing federal agency information and information systems.
E-Government Act of 2002	Enhances protection of personal information in government information systems by requiring that agencies conduct privacy impact assessments.
The Privacy Act of 1974	Places privacy restrictions on data collected by government agencies maintained in systems of records. Also requires agencies to secure and protect information using adequate technical and physical safeguards.
Health Insurance Portability and Accountability Act of 1996	Requires privacy regulations that establish standards for protecting medical records and other personal health information of individuals. Resulting regulations include encryption as an addressable (not required) implementation specification.
Veterans Benefits, Health Care, and Information Technology Act of 2006	Authorizes information technology security requirements for personally identifiable information at the Department of Veterans Affairs, including the requirement to develop procedures for detecting, reporting, and responding to security incidents.

Source: GAO analysis of key laws that frame protection of sensitive information.

[24] Pub. L. No. 109-461 (Dec. 22, 2006).

OMB Policy Requires Encryption of Sensitive Government Information on Mobile Devices

OMB is responsible for establishing governmentwide policies and for providing guidance to agencies on how to implement the provisions of FISMA, the Privacy Act, and other federal information security and privacy laws. OMB policy expands on the risk-based information security program requirements of FISMA in its 2002 and 2004 guidance[25] and in the wake of recent security breaches involving personal data, outlines minimum practices for implementation of encryption required by federal agencies in guidance issued in 2006 and 2007. Specifically

- OMB memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*, requires that agencies implement specific security controls recommended by NIST,[26] including the use of approved cryptographic techniques for certain types of electronic transactions that require a specified level of protection.
- OMB memorandum M-06-16, *Protection of Sensitive Agency Information*, recommends, among other things, that agencies encrypt all agency data on mobile computers and devices or obtain a waiver from the Deputy Secretary of the agency that the device does not contain sensitive information. The memorandum also recommends that agencies use a NIST checklist[27] provided in the memorandum that states agencies should verify that information requiring protection is appropriately categorized and assigned an appropriate risk impact category.
- OMB memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, restated the M-06-16 recommendations as requirements, and also required the use of NIST-certified cryptographic modules.

These OMB memorandums significant to the use of encryption are briefly described in table 3.

[25] OMB Memorandum 04-04 requires agencies with systems using remote authentication to conduct special electronic authentication risk assessments and select proper controls as recommended by NIST to protect sensitive information on those systems.

[26] NIST, Special Publication 800-63, *Electronic Authentication Guideline* (Gaithersburg, Maryland: April 2006).

[27] The checklist provided in M-06-16 provides specific actions to be taken by federal agencies for the protection of personally identifiable information categorized in accordance with FIPS 199 as moderate or high impact that is either accessed remotely or physically transported outside of the agency's secured physical perimeter. The security controls and associated control assessment methods/procedures in the checklist were taken from NIST Special Publication 800-53 and NIST Special Publication 800-53A.

Table 3: Major OMB Memorandums Related to the Use of Encryption

OMB memorandum	Description
*Reporting Instructions for the Government Information Security Reform Act and Updated Guidance on Security Plans of Action and Milestones, (*M-02-09), July 2, 2002	Requires that agencies document and track plans of actions and milestones necessary to implement security controls including the use of encryption if required
E-Authentication Guidance for Federal Agencies, (M-04-04), Dec. 16, 2003	Requires agencies with systems using remote authentication to conduct electronic authentication risk assessments and select proper controls, including the use of cryptographic components, as recommended by NIST, to protect sensitive information on those systems
Protection of Sensitive Agency Information, (M-06-16), June 23, 2006	Recommends that agencies encrypt all data on mobile computers/devices
Safeguarding Against and Responding to the Breach of Personally Identifiable Information, (M-07-16), May 22, 2007	Restates the recommendations of OMB M-06-16 as requirements and requires that agencies use NIST-certified cryptographic modules in encryption efforts

Source: GAO analysis of OMB memorandums on encryption.

NIST Provides Guidance and Standards for Encryption Use

In support of federal laws and policies, NIST provides federal agencies with implementation guidance and mandatory standards for identifying and categorizing information types and for selecting adequate controls based on risk, such as encryption, to protect sensitive information. Specifically, NIST Special Publication 800-53 instructs agencies to follow the implementation guidance detailed in supplemental NIST publications, including the following: [28]

- NIST Special Publication 800-21, *Guideline for Implementing Cryptography in the Federal Government*, guides the implementation of encryption by agencies. It recommends that prior to selecting a cryptographic method, or combination of methods, agencies address several implementation considerations when formulating an approach and developing requirements for integrating cryptographic methods into new or existing systems, including installing and configuring appropriate cryptographic components associated with selected encryption technologies; monitoring the continued effectiveness and functioning of

[28] NIST, Special Publication 800-53 Revision 2, *Recommended Security Controls for Federal Information Systems*, (Gaithersburg, Maryland: December 2007).

encryption technologies; developing policies and procedures for life cycle management of cryptographic components (such as procedures for management of encryption keys, backup and restoration of services, and authentication techniques); and training users, operators, and system engineers.

- Special Publication 800-57, *Recommendation for Key Management*, provides guidance to federal agencies on how to select and implement cryptographic controls for protecting sensitive information by describing cryptographic algorithms, classifying different types of keys used in encryption, and providing information on key management.

- Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, provides implementation guidance on the assignment of security categories to information and information systems using FIPS 199.[29]

- Special Publication 800-63, *Electronic Authentication Guideline*, addresses criteria for implementing controls that correspond to the assurance levels of OMB memorandum M-04-04 such that, if agencies assign a level 2, 3, or 4 to an electronic transaction, they are required to implement specific security controls, including the use of approved cryptographic techniques.

- Special Publication 800-77, *Guide to IPsec VPNs*, provides technical guidance to agencies in the implementation of virtual private networks, such as identifying needs and designing, deploying, and managing the appropriate solution, including the use of Federal Information Processing Standards (FIPS)-compliant encryption algorithms.

NIST also issues FIPS, which frame the critical elements agencies are required to follow to protect sensitive information and information systems. Specifically

- FIPS 140-2, *Security Requirements for Cryptographic Modules*.[30] Agencies are required to encrypt agency data, where appropriate, using NIST-certified cryptographic modules.[31] This standard specifies the security

[29] FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems* (Gaithersburg, Maryland: February 2004).

[30] Supersedes FIPS 140-1, 1994.

[31] OMB M-07-16.

requirements for a cryptographic module used within a security system protecting sensitive information in computer and telecommunication systems (including voice systems) and provides four increasing, qualitative levels of security intended to cover a wide range of potential applications and environments.

- Several standards describe the technical specifications for cryptographic algorithms, including those required when using digital signatures.[32]
- FIPS 199 provides agencies with criteria to identify and categorize all of their information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels.[33]
- FIPS 200 requires a baseline of minimum information security controls for protecting the confidentiality, integrity, and availability of federal information systems and the information processed, stored, and transmitted by those systems.[34] FIPS 200 directs agencies to implement the baseline control recommendations of NIST Special Publication 800-53. The following security-related areas in FIPS 200 whose controls are further detailed in Special Publication 800-53 pertain to the use of encryption:
    - *Access control*—describes controls for developing and enforcing policies and procedures for access control including remote access, wireless access, and for portable and mobile devices using mechanisms such as authentication and encryption.
    - *Contingency planning*—includes controls to ensure that the organization protects system backup information from unauthorized modification by employing appropriate mechanisms such as digital signatures.
    - *Identification and authentication*—describes controls for developing and documenting identification and authentication policies and procedures.

[32] FIPS 180-2, 186-3, and 197.

[33] FIPS 199.

[34] FIPS 200, *Minimum Security Requirements for Federal Information and Information System.* (Gaithersburg, Maryland: March 2006).

- *Maintenance*—includes remote maintenance control that addresses how an organization approves, controls, and monitors remotely executed maintenance and diagnostic activities including using encryption and decryption of diagnostic communications.

- *Media protection*—describes developing policies and procedures for media protection including media storage (which may include encrypting stored data) and transport.

- *System and communications protection*—includes controls to ensure the integrity and confidentiality of information in transit by employing cryptographic mechanisms if required, including establishing and managing cryptographic keys.

NIST publications pertaining to the use of encryption in federal agencies are briefly described in table 4.

Table 4: Key NIST Publications for Implementing Encryption Technology

NIST publication	Description
Guideline for Implementing Cryptography In the Federal Government (Special Publication 800-21)	Directs agencies on how to select and implement cryptographic controls for protecting sensitive information
Recommended Security Controls for Federal Information Systems (Special Publication 800-53, Revision 2)	Recommends that agencies select and specify security controls for information systems, including controls for implementing cryptographic components
Recommendation for Key Management (Special Publication 800-57)	Recommends technical guidance to agencies in the proper management and protection of cryptographic keys and the information associated with the keys
Guide for Mapping Types of Information and Information Systems to Security Categories (Special Publication 800-60, Revision 1)	Directs agencies to categorize information and information systems, helping agencies determine their needs for encryption
Electronic Authentication Guideline (Special Publication 800-63)	Directs agencies to properly implement electronic authentication,[a] including use of cryptographic components where required by the level of electronic authentication assurance
Guide to IPsec VPNs (Special Publication 800-77)	Directs agencies to properly implement virtual private networks, such as with the use of FIPS-compliant encryption algorithms

NIST publication	Description
Security Requirements for Cryptographic Modules (FIPS 140-2)	Requires agencies to employ this standard when designing and implementing cryptographic modules that federal agencies operate or are operated for them under contract
Secure Hash Standard (FIPS 180-2)	Mandates that agencies implement this standard whenever a secure hash algorithm is required for federal applications, including use by other cryptographic algorithms and protocols
Digital Signature Standard (FIPS 186-3)	Requires agencies to use this standard when designing and implementing public key-based signatures systems
Advanced Encryption Standard (FIPS 197)	Requires use of this or other FIPS-compliant cryptographic algorithms when an agency determines that sensitive (unclassified) information requires cryptographic protection
Standards for Security Categorization of Federal Information and Information Systems (FIPS 199)	Requires agencies to use risk-based criteria for the security categorization of information and information systems, helping agencies determine their needs for encryption
Minimum Security Requirements for Federal Information and Information Systems (FIPS 200)	Requires agencies to select and implement minimum information security controls based on risk

Source: GAO analysis of NIST publications.

[a] The process of electronically establishing confidence in a user's identity.

Efforts to Encrypt Sensitive Information Varied among Agencies

The extent to which 24 major federal agencies reported that they had implemented encryption and developed plans to implement encryption varied across agencies. Although all agencies had initiated efforts to encrypt stored and transmitted sensitive agency information, none had completed these efforts or developed and documented comprehensive plans to guide their implementation of encryption technologies. Our tests at 6 selected agencies revealed weaknesses in the encryption implementation practices involving the installation and configuration of FIPS-validated cryptographic modules encryption products, monitoring the effectiveness of installed encryption technologies, the development and documentation of policies and procedures for managing these technologies, and the training of personnel in the proper use of installed encryption products. As a result of these weaknesses, federal information may remain at increased risk of unauthorized disclosure, loss, and modification.

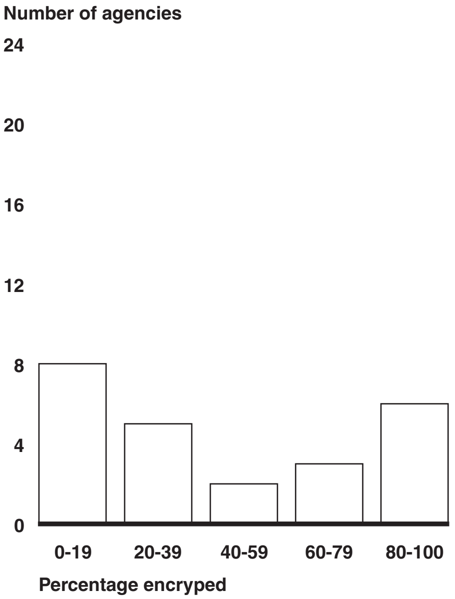
Reported Efforts to Encrypt Stored Information Lagged behind Efforts to Encrypt Transmitted Information

All 24 major federal agencies reported varying degrees of progress in their efforts to encrypt stored and transmitted sensitive agency information. While most of the agencies reported that they had not completed efforts to encrypt stored sensitive information, they reported being further along with efforts to encrypt transmitted sensitive information. Preparing for the implementation of encryption technologies involves numerous considerations. In response to our survey, agencies reported that they had encountered challenges that hinder the implementation of encryption. See appendix III for a discussion of the hindrances identified by agencies.

Few Agencies Have Encrypted All Sensitive Information Stored on Mobile Devices

OMB requires agencies to encrypt all agency data on mobile computers and devices or obtain a waiver from the Deputy Secretary of the agency stating that the device does not contain sensitive information. Of 24 agencies that reported from July through September 2007 on the status of their efforts to encrypt sensitive information stored on their laptops and handheld mobile devices, 8 agencies reported having encrypted information on less than 20 percent of these devices and 5 agencies reported having encrypted information on between 20 and 39 percent of these devices (see fig. 3). Overall, the 24 agencies reported that about 70 percent of laptop computers and handheld devices had not been encrypted.

Figure 3: Percentage of Encrypted Laptop Computers and Handheld Computing Devices at 24 Major Federal Agencies



Source: GAO analysis of agency-supplied data.

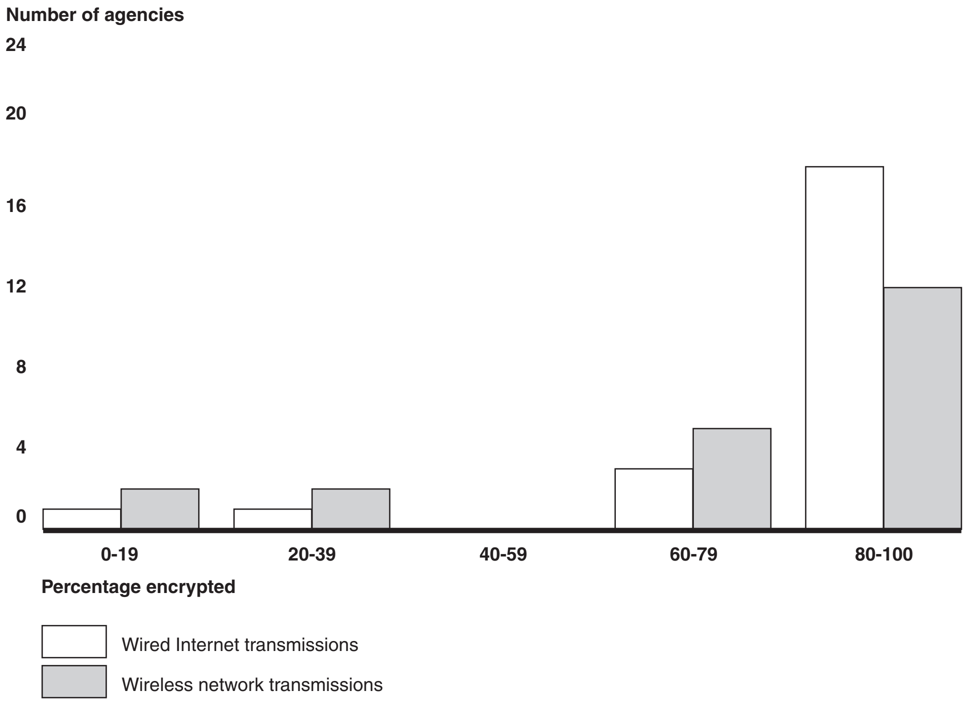
In addition, 10 of 22 agencies reported having encrypted information on less than 20 percent of portable storage media taken offsite, and 3 of 22 reported having encrypted between 20 and 39 percent. Further, 9 of 17 agencies reported encrypting sensitive information on less than 20 percent of offsite backup storage media. However, while agencies were encrypting sensitive data on mobile computers and devices such as laptop computers and handheld devices (e.g. personal digital assistants), 6 agencies reported having other storage devices, such as portable storage media, that could contain sensitive data. Of the 6 agencies, 4 had not encrypted these additional devices. Further, officials at 1 agency had no plans to encrypt sensitive data contained on their portable media.

In response to our query in April 2008, OMB officials stated that the term "mobile computers and devices" was intended to include all agency laptops, handheld devices, and portable storage devices such as portable drives and CD-ROMs that contain agency data. Nevertheless, this description is not clear in any of its memorandums. Until OMB clarifies the applicability of the encryption requirement so that agencies can complete encrypting sensitive agency information stored on applicable devices, the information will remain at risk of unauthorized disclosure.

Most Agencies Are Encrypting Sensitive Transmitted Information

Most agencies reported that they had encrypted sensitive information transmitted over wired and wireless networks. Of 23 agencies reporting on their efforts to encrypt wired Internet transmissions of sensitive information, 18 agencies reported encrypting nearly all or all (80 percent to 100 percent), of their transmissions over wired Internet networks. In addition, of 21 agencies reporting on their efforts to encrypt wireless transmissions of sensitive information, 12 reported having encrypted all or nearly all such transmissions (see fig. 4).

Figure 4: Agency Status of Encrypting Sensitive Information Transmitted Over Wired and Wireless Networks



Source: GAO analysis of survey data reported July through September 2007 by 21 agencies regarding encryption of sensitive information transmitted by wireless networks, and by 23 agencies regarding encrypting such information transmitted by the Internet.

Encryption Efforts Had Not Been Adequately Planned at Most Agencies

Although 24 major federal agencies reported having encryption efforts under way, none of the agencies had documented a comprehensive plan that considered the security control implementation elements recommended by NIST. According to NIST, cryptography is best designed as an integrated part of a comprehensive information security program rather than as an add-on feature and it suggests that implementing technical approaches without a plan to guide the process is the least effective approach to making use of cryptography. Specifically, as part of an effective information security program, NIST Special Publication 800-53 requires agencies to inventory and categorize information and systems according to risk as well as to document the baseline security controls—such as encryption—selected to adequately mitigate risks to information. However, of the 24 agencies we surveyed, 18 reported that they had not completed efforts to inventory sensitive information that they hold.

Further, NIST recommends that agencies follow NIST Special Publication 800-21 guidance when formulating their approach for integrating cryptographic methods into new or existing systems and documenting plans for implementing encryption, such plans consist of the following minimum elements:

- installing and properly configuring FIPS-validated cryptographic modules associated with selected encryption technologies;
- monitoring the continued effectiveness of installed cryptographic controls, including the proper functioning of encryption technologies;
- documenting and implementing policies and procedures for management of cryptographic components, such as the effective implementation and use of FIPS-compliant encryption technologies and the establishment and management of encryption keys; and
- providing training to users, operators, and system engineers.

Although several agencies had developed ad hoc encryption technology acquisition or deployment plans, none of the agencies had documented comprehensive plans that addressed the elements recommended by NIST.

In response to our query, OMB officials stated that they monitor agencies' progress toward implementing encryption through quarterly data submitted by the agencies as part of the President's Management Agenda scorecard. However, OMB did not provide us with evidence to demonstrate monitoring of the agencies' efforts to inventory the sensitive information they hold or to develop implementation plans. As previously noted, agencies did not have such plans and often did not have inventories. Until agencies develop and document comprehensive plans to guide their approach for implementing encryption, including completing an inventory of the sensitive information they hold, agencies will have limited assurance that they will be able to effectively complete implementation and manage life cycle maintenance of encryption technologies, as we observed at selected agencies and discuss later in this report.

Weaknesses in Encryption Implementation Practices Exist at Selected Agencies

Practices for implementing encryption displayed weaknesses at the 6 federal agencies we reviewed for testing.[35] Specifically, 2 of the 6 agencies had not installed FIPS-validated cryptographic modules encryption technologies and 4 had not configured installed encryption technologies in accordance with FIPS 140-2 specifications. In addition, all of the 6 agencies had not either developed or documented policies and procedures for managing encryption implementation, and 3 of these agencies had not adequately trained personnel in the effective use of installed encryption technologies. Protection of information and information systems relies not only on the technology in place but on establishing a foundation for effective implementation, life cycle management, and proper use of the technologies. Until agencies resolve these weaknesses, their data may not be fully protected.

FIPS-Compliant Encryption Products Had Not Been Installed on All Agency Devices

OMB requires agencies to protect sensitive agency data stored on mobile devices by installing a FIPS-validated cryptographic modules product, and NIST Special Publication 800-53 recommends that agencies install FIPS-compliant products when the agency requires encryption of stored or transmitted sensitive information. Agencies can now acquire FIPS-validated cryptographic module products for encrypting stored information through the General Services Administration's (GSA) SmartBUY program (see app. IV for a description of this program). Use of encryption technologies approved by NIST as compliant with FIPS 140-2 provides additional assurance that the product implemented—if configured correctly—will help protect sensitive information from unauthorized disclosure.

Laptop computers. The Department of Housing and Urban Development (HUD) had not installed encryption products on any of its laptop computers despite an agency official's assertions to the contrary. HUD officials explained that they had planned to implement FIPS-compliant encryption in fiscal year 2008 but that implementation was delayed until late in fiscal year 2008 due to lack of funding and it is now part of their fiscal year 2009 budget request. In addition, the Department of Education

[35] We selected six agencies that reported having initiated efforts to install FIPS-validated cryptographic modules encryption technologies on their laptop computers, BlackBerry® devices, or virtual private networks or that had either experienced publicized incidents of data compromise or were expected to collect, store, and transmit a wide range of sensitive information. The six agencies are the General Services Administration; the Departments of Education, Agriculture, Housing and Urban Development, and State; and the National Aeronautics and Space Administration.

had not installed a FIPS-validated cryptographic modules product to encrypt sensitive information on any of the 15 laptop computers that we tested at one of its components. Of the 4 remaining agencies, 3—the Department of Agriculture (USDA), the State Department,[36] and GSA—had installed FIPS-compliant technologies on all 58 of the laptop computers that we tested at specific locations within each agency. At the National Aeronautics and Space Administration (NASA) location we tested, we confirmed that the agency's selected FIPS-compliant encryption software had been installed on 27 of 29 laptop computers. Although the agency asserted that it had installed it on all 29 laptops, officials explained that they did not have a mechanism to detect whether the encryption product was successfully installed and functioning.

Handheld devices. All 6 of the agencies had deployed FIPS-compliant handheld mobile devices (specifically, BlackBerry® devices) for use by personnel. BlackBerry software and the BlackBerry enterprise server software enable users to store, send, and receive encrypted e-mail and access data wirelessly using FIPS-validated cryptographic modules encryption algorithms.

Virtual private networks. One of three virtual private networks installed by the Department of Education was not a FIPS-compliant product. The remaining 5 agencies had installed FIPS-validated cryptographic modules products to protect transmissions of sensitive information.

Certain Agencies Did Not Consistently Configure or Install Encryption Technologies in Accordance with NIST Requirements

Although most agencies had installed FIPS-compliant products to encrypt information stored on devices and transmitted across networks, some did not monitor whether the product was functioning or configure the product to operate only in a FIPS-validated cryptographic modules secure mode. Until agencies configure FIPS-compliant products in a secure mode as

[36] We were unable to test the installation of encryption products on deployed laptops assigned to State employees because although the inventory provided by the agency indicated that the employees were assigned to the location that we visited, they were actually assigned to posts throughout the world. We instead discussed the encryption installation process with State officials and verified use of a FIPS-validated cryptographic modules product on one unassigned laptop (not from our sample) that agency officials provided for our examination. Officials stated that the laptop inventory provided for our review included only those laptop computers that were assigned for telecommuting and that it did not constitute the entire universe of State's laptops. A State official asserted that all of the telecommuting laptops—about 2,100 in total—were encrypted as a condition for assigning the device to a telecommuting employee and that approximately 19 percent of their remaining laptops were encrypted.

directed by NIST—for example, by enabling only FIPS-validated cryptographic module encryption algorithms—protection against unauthorized decryption and disclosure of sensitive information will be diminished.

Laptop computers. Of the 4 agencies with FIPS-compliant products installed on laptop computers, 3 had configured the product to operate in a secure mode as approved by NIST on all devices that we examined. However, a component of the Department of Agriculture had not effectively monitored the effectiveness and continued functioning of encryption products on 5 of the 52 laptop computers that we examined. Agency officials were unaware that the drives of these devices had not been correctly encrypted. The drives, while having the encryption software installed, did not encrypt the data on the drive. This agency's system administrator attributed the noncompliance to the failure of a step in the installation process; specifically, the laptop had not been connected to the agency's network for a sufficient period of time to complete activation of the user's encryption key by the central server, and the agency had no mechanism in place to monitor whether the installed product was functioning properly.

Handheld devices. Three of the 6 agencies—the Department of Education, HUD, and NASA—had not configured their handheld BlackBerry devices to encrypt the data contained on the devices. All six of the agencies encrypted data in transit because FIPS-validated cryptographic modules encryption was built into the BlackBerry device software. However, agencies must enable the encryption to protect information stored on the device itself by making a selection to do so and requiring the user to input a password. Officials at these 3 agencies stated that they had not enabled this protective feature on all their BlackBerry devices due to operational issues with enabling content protection and that they are awaiting a solution from the vendor.

Virtual private networks. Two of the 6 agencies—the Department of Education and HUD—had not configured their virtual private networking technologies to use only strong, FIPS-validated cryptographic modules encryption algorithms for encrypting data and to ensure message integrity. The use of weak encryption algorithms—ones that have not been approved by NIST or that have explicitly been disapproved by NIST—provides limited assurance that information is adequately protected from unauthorized disclosure or modification.

Agencies Had Not Developed or Documented Encryption Policies and Procedures

The weaknesses in encryption practices identified at the 6 selected agencies existed in part because agencywide policies and procedures did not address federal guidelines related to implementing and using encryption. NIST Special Publication 800-53 recommends that agencies develop a formal, documented policy that addresses the system and communications controls as well as a formal, documented procedure to facilitate implementation of these controls. While policies should address the agency's position regarding use of encryption and management of encryption keys, the implementation procedures should describe the steps for performance of specific activities such as user registration, system initialization, encryption key generation, key recovery, and key destruction. However, 4 of the 6 agencies did not have a policy that addressed the establishment and management of cryptographic keys as directed by NIST, and none of the 6 agencies had detailed procedures for implementing this control.

Furthermore, according to NIST guidance, agency policies and procedures are to address how agencies will install and configure FIPS-compliant encryption products. All agencies' policies addressed how the agency planned to comply with these requirements. However, 4 agencies did not have detailed procedures requiring installation and configuration of FIPS-compliant cryptography (see table 5).

Table 5: Agency Policies and Procedures That Address NIST Encryption Controls

	Encryption key establishment and management control		Installation and donfiguration of FIPS-compliant encryption products	
Agency	Policy	Procedures	Policy	Procedures
USDA	Yes	No	Yes	Yes
Education	No	No	Yes	No
HUD	Yes	No	Yes	No
State	No	No	Yes	No
GSA	No	No	Yes	No
NASA	No	No	Yes	Yes

Source: GAO analysis of agency policies and procedures for NIST encryption controls.

Policies and procedures for installing and configuring encryption technologies and for managing encryption keys provide the foundation for the effective implementation and use of encryption technologies and are a necessary element of agency implementation plans. Until these agencies develop, document, and implement these policies and procedures, the agencies' implementation of encryption may be ineffective in protecting the confidentiality, integrity, and availability of sensitive information.

Three Agencies Had Not Adequately Trained Personnel to Use Installed Encryption Products

Also contributing to the weaknesses at 3 of 6 agencies was the failure to adequately train personnel in the proper use of installed encryption technology. Specifically

- USDA officials stated that users had not been trained to check for continued functioning of the software after installation but that they were in the process of including encryption concepts in its annual security awareness training required for all computer users. At the conclusion of our review, USDA had not yet completed this effort.

- At the component of the Department of Education where testing was conducted, some users were unaware that the agency had installed encryption software on their laptop computers. These users, therefore, had never used the software to encrypt sensitive files or folders. Further, while an agency official asserted that encryption training was provided, the training documents provided pertained only to the protection of personally identifiable information and did not provide specifics on how to use the available encryption products. Users we spoke with were unaware of any available training.

- At NASA, several users stated that they had refused to allow the encryption software to be installed on their devices, while other users said they were unfamiliar with the product. Although NASA requires users to receive training when encryption is installed and has developed a training guide, there was no mechanism in place to track whether users complete the necessary training.

Until these agencies provide effective training to their personnel in the proper management and use of installed encryption technologies, they will have limited confidence in the ability of the installed encryption technologies to function as intended.

Conclusions

Despite the availability of numerous types of commercial encryption technologies and federal policies requiring encryption, most federal agencies had just begun to encrypt sensitive information on mobile computers and devices. In addition, agencies had not documented comprehensive plans to guide activities for effectively implementing encryption. Although governmentwide efforts were under way, agency uncertainty with OMB requirements hampered progress. In addition, weaknesses in encryption practices at six selected federal agencies—including practices for installing and configuring FIPS-validated cryptographic modules products, monitoring the effectiveness of these technologies, developing encryption policies and procedures, and training personnel—increased the likelihood that the encryption technologies used by the agencies will not function as intended. Until agencies address these weaknesses, sensitive federal information will remain at increased risk of unauthorized disclosure, modification, or loss.

Recommendations for Executive Action

We are making 20 recommendations to the Director of the Office of Management and Budget and six federal departments and agencies to strengthen encryption of federal systems.

To assist agencies with effectively planning for and implementing encryption technologies to protect sensitive information, we recommend that the Director of the Office of Management and Budget take the following two actions:

- clarify governmentwide policy requiring agencies to encrypt sensitive agency data through the promulgation of additional guidance and/or through educational activities and
- monitor the effectiveness of the agencies' encryption implementation plans and efforts to inventory the sensitive information they hold.

To assist the Department of Agriculture as it continues to deploy its departmentwide encryption solutions and to improve the life cycle management of encryption technologies, we recommend that the Secretary of Agriculture direct the chief information officer to take the following three actions:

- establish and implement a mechanism to monitor the successful installation and effective functioning of encryption products installed on devices,
- develop and implement departmentwide procedures for encryption key establishment and management, and
- develop and implement a training program that provides technical support and end-user personnel with adequate training on encryption concepts, including proper operation of the specific encryption products used.

We also recommend that the Secretary of the Department of Education direct the chief information officer to take the following five actions to improve the life cycle management of encryption technologies:

- evaluate, select, and install FIPS 140-compliant products for all encryption needs and document a plan for implementation that addresses protection of all sensitive information stored and transmitted by the agency;
- configure installed FIPS-compliant encryption technologies in accordance with FIPS-validated cryptographic modules security settings for the product;
- develop and implement departmentwide policy and procedures for encryption key establishment and management;
- develop and implement departmentwide procedures for use of FIPS-compliant cryptography; and
- develop and implement a training program that provides technical support and end-user personnel with adequate training on encryption concepts, including proper operation of the specific encryption products used.

To ensure that the Department of Housing and Urban Development is adequately protecting its sensitive information and to improve the life cycle management of encryption technologies at the department, we recommend that the Secretary of Housing and Urban Development direct the chief information officer to take the following three actions:

- evaluate, select, and install FIPS 140-compliant products for all encryption needs and document a plan for implementation that addresses protection of all sensitive information stored and transmitted by the agency;
- configure installed FIPS-compliant encryption technologies in accordance with FIPS-validated cryptographic modules security settings for the product; and
- develop and implement departmentwide procedures for the use of FIPS-compliant cryptography and for encryption key establishment and management.

To improve the life cycle management of encryption technologies at the Department of State, we recommend that the Secretary of State direct the chief information officer to take the following two actions:

- develop and implement departmentwide policy and procedures for encryption key establishment and management and

- develop and implement departmentwide procedures for use of FIPS-compliant cryptography.

To improve the life cycle management of encryption technologies at the General Services Administration, we recommend that the Administrator of the General Services Administration direct the chief information officer to take the following two actions:

- develop and implement departmentwide policy and procedures for encryption key establishment and management and

- develop and implement departmentwide procedures for use of FIPS-compliant cryptography.

As the National Aeronautics and Space Administration continues to plan for a departmentwide encryption solution and to improve the life cycle management of encryption technologies, we recommend that the Administrator of the National Aeronautics and Space Administration direct the chief information officer to take the following three actions:

- establish and implement a mechanism to monitor the successful installation and effective functioning of encryption products installed on devices,

- develop and implement departmentwide policy and procedures for encryption key establishment and management, and

- develop and implement a training program that provides technical support and end-user personnel with adequate training on encryption concepts, including proper operation of the specific encryption products used.

Agency Comments

We received written comments on a draft of this report from the Administrator, Office of E-Government and Information Technology at OMB (reproduced in app. V). OMB generally agreed with the report's contents and stated that it would carefully consider our recommendations. We also received written comments from Education's Chief Information Officer (reproduced in app. VI), from HUD's Acting Chief Information Officer (reproduced in app. VII), from the Department of State (reproduced in app. VIII), from the Acting Administrator of the GSA (reproduced in app. IX), and from the Deputy Administrator of NASA (reproduced in app. X). We received comments via email from the Department of Agriculture.

In these comments, the Departments of Agriculture, Education, HUD, and State; the GSA; and NASA agreed with our recommendations to their respective departments. Agencies also stated that they had implemented or were in the process of implementing our recommendations. In addition, NIST and the Social Security Administration provided technical comments, which we have incorporated as appropriate.

As we agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution of it until 30 days from the date of this letter. At that time, we will send copies of this report to interested congressional committees and the agency heads and inspectors general of the 24 major federal agencies. We will also make copies available to others on request. In addition, this report will be available at no charge on the GAO Web site at http://www.gao.gov.

If you have any questions or wish to discuss this report, please contact me at (202) 512-6244 or wilshuseng@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix XI.

Gregory C. Wilshusen

Gregory C. Wilshusen
Director, Information Security Issues

Appendix I: Objectives, Scope, and Methodology

The objectives of our review were to determine (1) how commercially available encryption technologies could help federal agencies protect sensitive information and reduce risks; (2) the federal laws, policies, and guidance for using encryption technologies to protect sensitive information; and (3) the extent to which agencies have implemented, or planned to implement, encryption technologies to protect sensitive information.

To address the first objective, we reviewed prior GAO reports and reviewed documentation regarding products validated by the National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program to identify commercially available encryption technologies. Additionally, we met with a vendor of an encryption product and interviewed NIST encryption experts regarding the characteristics of products that can reduce risks to agencies.

To address the second objective, we reviewed prior GAO and agency inspector general reports to identify relevant laws and guidance such as the Federal Information Security Management Act of 2002 (FISMA) and the Privacy Act of 1974 to identify mandatory and optional practices for protecting sensitive information (including personally identifiable information but excluding classified national security information) that federal agencies collect, process, store, and transmit. We examined the laws to identify federal agencies responsible for promulgating federal policies and standards on the use of encryption. Additionally, we researched official publications issued by the Office of Management and Budget and NIST and interviewed officials from these agencies to identify the policies, standards, and guidance on encryption that have been issued.

To address the third objective, we collected and analyzed agency-specific policies, plans, and practices through a data request and also conducted a survey of the 24 major federal agencies. A survey specialist designed the survey instrument in collaboration with subject matter experts. Then, the survey was pretested at 4 of these agencies to ensure that the questions were relevant and easy to comprehend. For each agency surveyed, we identified the appropriate point of contact, notified each one of our work, and distributed the survey along with a data request to each via e-mail in June 2007. In addition, we discussed the purpose and content of the survey and data request with agency officials when requested. All 24 agencies responded to our survey and data request from June to September 2007; results are reported as of this date. We contacted agency officials when necessary for additional information or clarification of agencies' status of encryption implementation. We did not verify the accuracy of the agencies' responses; however, we reviewed supporting documentation that agencies provided to corroborate information provided in their responses. We then analyzed the results from the survey and data request to identify:

- the types of information encrypted in data when stored and in transit;
- technologies used by the agency to encrypt information;
- whether the technologies implemented by the agency met federal guidelines;
- the extent to which the agency has implemented, or plans to implement, encryption; and
- any challenges faced and lessons learned by agencies in their efforts to encrypt sensitive but unclassified information.

Conducting any survey may introduce errors. For example, differences in how a particular question is interpreted, the sources of information that are available to respondents, or how the data are entered or were analyzed can introduce variability into the survey results. We took steps in the development of the survey instrument, the data collection, and the data analysis to minimize errors.

In addition, we tested the implementation of encryption technologies at 6 agencies to determine whether each agency was complying with federal guidance that required agencies to use NIST-validated encryption technology. Out of 24 major federal agencies, we selected 6 that met one or more of the following conditions: they (1) had not been tested under a recent GAO engagement, (2) had reported having initiated efforts to install FIPS-validated cryptographic modules encryption technologies, (3) had experienced publicized incidents of data compromise, or (4) were reasonably expected to collect, store, and transmit a wide range of sensitive information. Specifically, we tested the implementation of encryption for BlackBerry servers, virtual private networks, or a random selection of laptop computers at specific locations at the following 6 agencies within the Washington, D.C. area: [1]

- U.S. Department of Agriculture,
- Department of Education,
- Department of Housing and Urban Development,
- Department of State,[2]
- General Services Administration, and
- National Aeronautics and Space Administration

At each of these agencies, we requested an inventory of laptop computers that were located at agency facilities in the Washington, D.C., metro area and that were encrypted. For each agency, we nonstatistically selected one location at which to perform testing, and thus the encryption test results for each agency cannot be projected to the entire agency. We performed the testing between September and December 2007. At each location where laptop computers were tested, there were a small number of laptop computers that were requested as part of our sample but which were not made available to us for testing. Department officials cited several reasons for this, including that the user of the device could not bring it to the location in time for our testing.

In testing the laptop computers, we determined whether encryption software had been installed on the device and whether the software had been configured properly to adhere to federally required standards. Although we identified unencrypted laptop computers at each agency, we were not able to make statistical estimates of the percentage of unencrypted devices at each location. The small number of devices in each

[1] We conducted testing at the headquarters locations of the Departments of Housing and Urban Development and State, the General Services Administration, and the National Aeronautics and Space Administration. We conducted testing at the Food and Nutrition Service component of the U.S. Department of Agriculture and at the Federal Student Aid component of the Department of Education.

[2] At the Departments of Housing and Urban Development and State, we tested only the BlackBerry server and virtual private networks.

sample not made available to us for our testing compromised the randomness of each sample.

Additionally, for each of the selected locations among the 6 agencies, we requested information on their BlackBerry servers, chose the server with the greatest number of users for testing, and reviewed through observation the specific security configuration settings. We also requested and examined agency-provided information for their virtual private networks to determine if encrypted networks were using products validated by NIST. Finally, we interviewed agency officials regarding their practices for encrypting stored data as well as data in transit, and for encryption key establishment and management.

Furthermore, we reviewed and analyzed data on the General Services Administration's SmartBUY program to determine the extent of savings the program provides to federal agencies and how certain agencies have already benefited from the program.

We conducted this performance audit from February 2007 through June 2008 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Important Considerations for Implementing Encryption to Effectively Reduce Agency Risks

Encryption technology may help protect sensitive information from compromise; however, there are several important implementation and management considerations when selecting and implementing this technology. Encryption can be a powerful tool, but implementing it incorrectly—such as by failing to properly configure the product, secure encryption keys, or train users—can, at best, result in a false sense of security and, at worst, render data permanently inaccessible. Designing, building, and effectively implementing commercially available cryptographic technologies involves more than installing the technology. Decisions must be made for managing encryption keys and related cryptographic components, as well as for managing mobile devices and using public key infrastructure (PKI) technologies. Ultimately, the effectiveness of the encryption technologies used to protect agency information and reduce risk depends on how an agency implements and manages these technologies and the extent to which they are an integral part of an effectively enforced information security policy that includes sound practices for managing encryption keys.

Encryption Key Management Considerations

Policies and procedures. Comprehensive policies for the management of encryption and decryption keys—the secret codes that lock and unlock the data—are an important consideration. Providing lifetime management of private keys and digital certificates across hundreds of applications and thousands of servers, end-users, and networked devices can quickly strain an agency's resources. For example, if a key is lost or damaged, it may not be possible to recover the encrypted data. Therefore, it is important to ensure that all keys are secured and managed properly by planning key management processes, procedures, and technologies before implementing storage encryption technologies. According to NIST, this planning would include all aspects of key management, including key generation, use, storage, and destruction. It would also include a careful consideration of how key management practices can support the recovery of encrypted data if a key is inadvertently destroyed or otherwise becomes unavailable (for instance, because a user unexpectedly resigns or loses a cryptographic token containing a key). An example of recovery preparation is storing duplicates of keys in a centralized, secured key repository or on physically secured removable media. Additional considerations for the encryption of removable media are how changing keys may affect access to encrypted storage on the media and what compensating controls could be developed, such as retaining the previous keys in case they are needed.

Key storage location. Another consideration that NIST describes is deciding where the local keys will be stored. For some encryption technologies, such as full disk encryption and many file/folder encryption products, there are often several options for key location, including the local hard drive, a flash drive, a cryptographic token, or a trusted platform module chip. Some products also permit keys to be stored on a centralized server and retrieved automatically after the user authenticates successfully. For virtual disk encryption, the main encryption key is often stored encrypted within the disk or container itself.

Access to encryption keys. Another consideration is properly restricting access to encryption keys. According to NIST, storage encryption technologies should require the use of one or more authentication mechanisms, such as passwords, smart cards, and cryptographic tokens, to decrypt or otherwise gain access to a storage encryption key. The keys themselves should be logically secured (encrypted) or physically secured (stored in a tamper-resistant cryptographic token). The authenticators used to retrieve keys should also be secured properly.

Managing cryptographic components related to encryption keys. In addition to key management, NIST describes several other considerations when planning a storage encryption technology. Setting the cryptography policy involves choosing the encryption algorithm, mode of cryptographic operation, and key length. Federal agencies must also use NIST-validated cryptographic modules configured for FIPS-compliant algorithms and key lengths. In addition, several FIPS-compliant algorithms are available for integrity checking. Another consideration for managing cryptographic components is how easily an encryption product can be updated when stronger algorithms and key sizes become available in the future.

Other Implementation Considerations

Centralized management of mobile devices. NIST recommends centralized management for most storage encryption deployments because of its effectiveness and efficiency for policy verification and enforcement, key management, authenticator management, data recovery, and other management tasks. Centralized management can also automate these functions: deployment and configuration of storage encryption software to end user devices, distribution and installation of updates, collection and review of logs, and recovery of information from local failures.

PKI technology. Because PKI technology uses a public key as part of its encryption system, PKI systems with key management can be used to avoid the problem of lost keys. Data encrypted with PKI relies on one public key, so the private key of the person encrypting the data isn’t necessarily required to decrypt it. However, if an unauthorized user is able to obtain a private key, the digital certificate could then be compromised. Agencies considering PKI technology must ensure that the key systems of different agencies are compatible for cross-agency collaboration on tasks such as security incident information sharing. Further, users of certificates are dependent on certification authorities to verify the digital certificates. If a valid certification authority is not used, or a certification authority makes a mistake or is the victim of a cyber attack, a digital certificate may be ineffective.

Ongoing maintenance of encryption technologies. Systems administrators responsible for encryption technology maintenance should be able to configure and manage all components of the technology effectively and securely. According to NIST, it is particularly important to evaluate the ease of deployment and configuration, including how easily the technology can be managed as the technology is scaled to larger deployments. Another consideration is the ability of administrators to disable configuration options so that users cannot circumvent the intended security. Other maintenance considerations NIST describes include the effects of patching/upgrading software, changing software settings (changing cryptographic algorithms or key sizes), uninstalling or disabling encryption software, changing encryption/decryption keys, and changing user or administrator passwords.

Appendix III: Hindrances Faced by Agencies when Implementing Encryption

Preparing an agency for encryption presents numerous challenges to agencies, including selecting an adequate combination of cost-effective baseline security controls, properly configuring the networks and user devices within the information technology (IT) infrastructure to accommodate selected encryption technologies, providing training to personnel, and managing encryption keys. In response to our survey, agencies reported several conditions that hinder their ability to encrypt sensitive information as required by the Office of Management and Budget.

In response to our survey, all 24 agencies reported hindrances with implementing encryption. These hindrances included prohibitive costs; user acceptance; user training; data backup and recovery; data archival and retrieval; interoperability; infrastructure; vendor support for encryption products acquired; availability of FIPS-compliant products to meet the needs of uncommon or unique devices, applications, or environments within the agency's IT infrastructure; and management support for migration to encryption controls. Agencies noted the level of hindrance caused by these challenges ranged from little or no hindrance to great or very great hindrance. The most challenging conditions are discussed below.

Prohibitive costs. Nine agencies reported that the cost of acquiring and implementing encryption was their greatest hindrance, and 13 agencies cited this condition as somewhat of a hindrance or a moderate hindrance. As reported in appendix IV, a governmentwide initiative (SmartBUY) has been established to assist agencies with overcoming this hindrance.

User acceptance and training. Some encryption technologies can be burdensome to users and can require specialized training on encryption concepts and proper installation, maintenance, and use of encryption products. Sixteen agencies reported facing somewhat of a hindrance or a moderate hindrance in obtaining user acceptance of encryption implementations and in training personnel. Four agencies reported a great or very great hindrance from lack of user acceptance, and 2 agencies reported a great hindrance from insufficient training.

Data backup, recovery, archiving, and retrieval. Agencies must establish policies and procedures for management of encryption keys, which are necessary to recover data from back-ups in the event of a service interruption or disaster, or to retrieve data in archived records, perhaps many years in the future. For example, if the key is not properly backed up and is on a server that has been destroyed in a fire or the key used to encrypt archived records changes over time, data encrypted with the key may be irretrievably lost. Sixteen agencies reported facing somewhat of a hindrance or a moderate hindrance with backup and recovery, and 15 agencies reported the same level of hindrance with data archiving and retrieval.

Interoperability. Key systems and technologies of different agencies need to be compatible with each other for cross-agency collaboration. Five agencies reported that lack of interoperability was a great or very great hindrance, and 13 reported somewhat of a hindrance or a moderate hindrance.

Infrastructure considerations. Six agencies reported facing a great or very great hindrance in readying their IT infrastructure for encryption and 11 reported this was somewhat of a hindrance or a moderate hindrance.

Table 6 summarizes the number of agencies reporting the extent to which 10 conditions affect their agency's ability to implement encryption.

Table 6: Hindrances to Implementing Encryption at Federal Agencies

Hindrance	Little or no hindrance	Some hindrance	Moderate hindrance	Great or very great hindrance
Prohibitive costs	2	8	5	9
Lack of user acceptance	3	12	4	4
Difficulties with data backup and recovery	5	10	6	3
Insufficient training	4	13	3	2
Difficulties with archiving and retrieving	5	12	3	3
Lack of interoperability	3	6	7	5
Lack of infrastructure readiness	7	2	9	6
Lack of vendor support	8	8	6	1
Lack of FIPS-compliant products	7	6	4	4
Lack of management acceptance	7	9	1	2

Source: GAO analysis of agency-reported data. Respondents were permitted to select more than one condition.

Although agencies reported facing hindrances to implementing encryption, a new program (GSA SmartBUY specific to encryption products) established after we started our review, offers agencies options to overcome key hindrances. For example, prohibitive costs and acquiring FIPS-compliant products are two hindrances that agencies may be able to address through SmartBUY. As discussed in appendix IV, discounted pricing is available for data-at-rest encryption software. In addition, all products available through SmartBUY use cryptographic modules validated under FIPS 140-2 security requirements.

Appendix IV: GSA SmartBUY Program for Data-at-Rest Encryption Products

To help agencies comply with OMB requirements for encrypting information on mobile devices, a governmentwide acquisition vehicle was established for encryption products for stored data. Through a governmentwide program known as SmartBUY (Software Managed and Acquired on the Right Terms), agencies can procure encryption software at discounted prices. According to the General Services Administration (GSA), SmartBUY is a federal government procurement vehicle designed to promote effective enterprise-level software management. By leveraging the government's immense buying power, SmartBUY could save taxpayers millions of dollars through governmentwide aggregate buying of commercial off-the-shelf software products.

SmartBUY officially began in 2003, when OMB issued a memo emphasizing the need to reduce costs and improve quality in federal purchases of commercial software. [1] The memo designates GSA as the executive agent to lead the interagency initiative in negotiating governmentwide enterprise licenses for software. SmartBUY establishes strategic enterprise agreements with software publishers (or resellers) via blanket purchase agreements.

OMB Memorandum 04-08, *Maximizing Use of SmartBUY and Avoiding Duplication of Agency Activities with the President's 24 E-Gov Initiatives*, requires agencies to review SmartBUY contracts to determine whether they satisfy agency needs—such as for products to encrypt stored data—and, absent a compelling justification for doing otherwise, acquire their software requirements from the SmartBUY program.

The issuance of OMB's May 2006 recommendation to encrypt mobile devices contributed to the addition of 11 SmartBUY agreements for stored data encryption products established in June 2007. The products offered fall into one of three software and hardware encryption product categories: full disk encryption, file encryption, or integrated full disk/file encryption products. All products use cryptographic modules validated under FIPS 140-2 security requirements.

Volume discounts on encryption products are available when purchasing in tiers of 10,000, 33,000, and 100,000 users. Each of the 11 agreements has its own pricing structure, which may include maintenance and training in

[1] OMB, *Reducing Cost and Improving Quality in Federal Purchases of Commercial Software* (M-03-14), (Washington, D.C.; June 2, 2003).

addition to licenses for users. Discounts on volume pricing can range up to 85 percent off GSA schedule prices.

Table 7 provides an example of the discounted pricing available from 1 of the 11 SmartBUY agreements for encryption software.

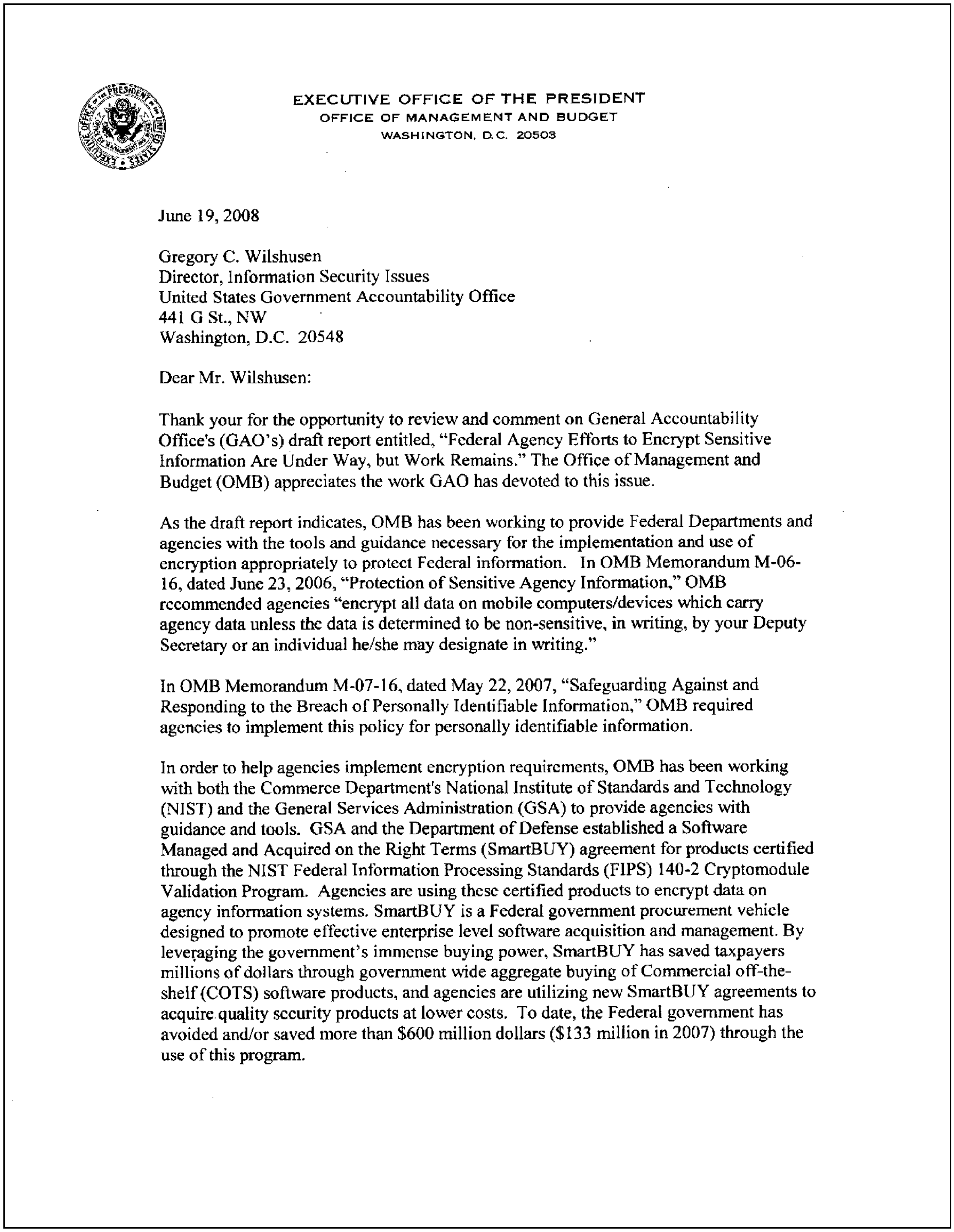
Table 7: Examples of Volume Discount Pricing Available through SmartBUY

Order quantity		Commercial list price	GSA schedule price	SmartBUY price
1-	99	$199.00	$171.08	$133.52
100-	499	164.00	140.99	102.47
500-	999	149.00	128.10	94.19
1,000-	1,999	133.00	114.34	81.77
2,000-	2,999	119.00	102.31	76.59
3,000-	4,999	111.00	$95.43	71.42
5,000-	9,999	98.00		67.50
10,000-	24,999	$83.00		54.75
25,000-	49,999			44.00
50,000-	99,999			37.00
100,000-	199,999			$30.00

Source: GSA supplied documentation.

As of January 2008, 10 agencies had purchased encryption products—such as software licenses, annual maintenance services, and training—from the stored data SmartBUY list, realizing significant cost savings. One of those agencies—the Social Security Administration—purchased 250,000 licenses of one of the stored data products at a savings of $6.7 million off the GSA schedule prices. Additionally, USDA negotiated an agreement for 180,000 licenses at $9.63 each, as opposed to the GSA unit price of $170 per license. The large number of licenses acquired allowed USDA to negotiate the low price. Several agencies noted that considering an enterprisewide deployment of encryption can be helpful with issues of standardization, interoperability, and infrastructure readiness. While 10 agencies have already acquired encryption products through the SmartBUY program, several agencies are still in the process of assessing which encryption products (including those available under the SmartBUY program) will best suit agency needs.

Appendix V: Comments from the Office of Management and Budget



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

June 19, 2008

Gregory C. Wilshusen
Director, Information Security Issues
United States Government Accountability Office
441 G St., NW
Washington, D.C. 20548

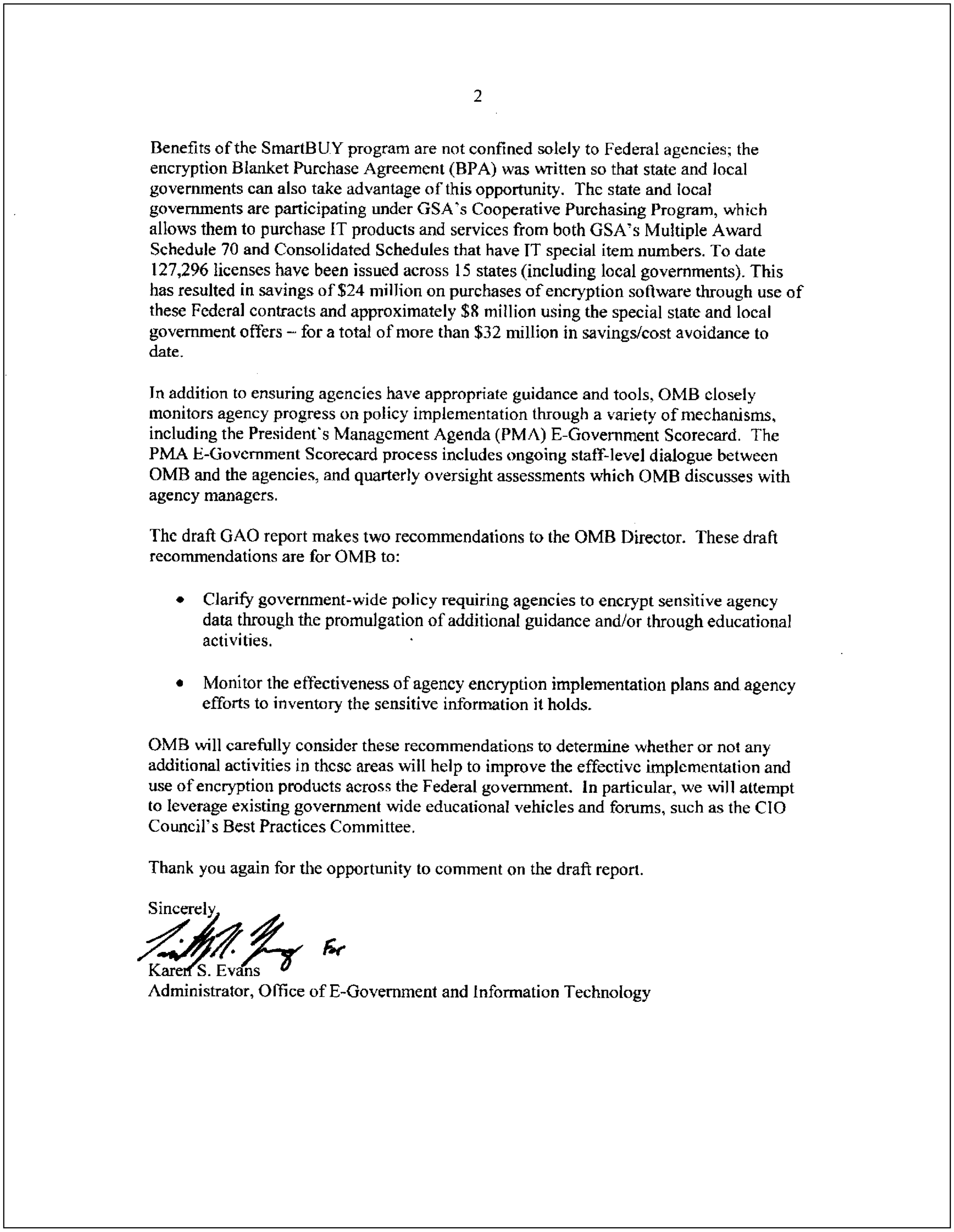
Dear Mr. Wilshusen:

Thank your for the opportunity to review and comment on General Accountability Office's (GAO's) draft report entitled, "Federal Agency Efforts to Encrypt Sensitive Information Are Under Way, but Work Remains." The Office of Management and Budget (OMB) appreciates the work GAO has devoted to this issue.

As the draft report indicates, OMB has been working to provide Federal Departments and agencies with the tools and guidance necessary for the implementation and use of encryption appropriately to protect Federal information. In OMB Memorandum M-06-16, dated June 23, 2006, "Protection of Sensitive Agency Information," OMB recommended agencies "encrypt all data on mobile computers/devices which carry agency data unless the data is determined to be non-sensitive, in writing, by your Deputy Secretary or an individual he/she may designate in writing."

In OMB Memorandum M-07-16, dated May 22, 2007, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," OMB required agencies to implement this policy for personally identifiable information.

In order to help agencies implement encryption requirements, OMB has been working with both the Commerce Department's National Institute of Standards and Technology (NIST) and the General Services Administration (GSA) to provide agencies with guidance and tools. GSA and the Department of Defense established a Software Managed and Acquired on the Right Terms (SmartBUY) agreement for products certified through the NIST Federal Information Processing Standards (FIPS) 140-2 Cryptomodule Validation Program. Agencies are using these certified products to encrypt data on agency information systems. SmartBUY is a Federal government procurement vehicle designed to promote effective enterprise level software acquisition and management. By leveraging the government's immense buying power, SmartBUY has saved taxpayers millions of dollars through government wide aggregate buying of Commercial off-the-shelf (COTS) software products, and agencies are utilizing new SmartBUY agreements to acquire quality security products at lower costs. To date, the Federal government has avoided and/or saved more than $600 million dollars ($133 million in 2007) through the use of this program.



2

Benefits of the SmartBUY program are not confined solely to Federal agencies; the encryption Blanket Purchase Agreement (BPA) was written so that state and local governments can also take advantage of this opportunity. The state and local governments are participating under GSA's Cooperative Purchasing Program, which allows them to purchase IT products and services from both GSA's Multiple Award Schedule 70 and Consolidated Schedules that have IT special item numbers. To date 127,296 licenses have been issued across 15 states (including local governments). This has resulted in savings of $24 million on purchases of encryption software through use of these Federal contracts and approximately $8 million using the special state and local government offers – for a total of more than $32 million in savings/cost avoidance to date.

In addition to ensuring agencies have appropriate guidance and tools, OMB closely monitors agency progress on policy implementation through a variety of mechanisms, including the President's Management Agenda (PMA) E-Government Scorecard. The PMA E-Government Scorecard process includes ongoing staff-level dialogue between OMB and the agencies, and quarterly oversight assessments which OMB discusses with agency managers.

The draft GAO report makes two recommendations to the OMB Director. These draft recommendations are for OMB to:

- Clarify government-wide policy requiring agencies to encrypt sensitive agency data through the promulgation of additional guidance and/or through educational activities.

- Monitor the effectiveness of agency encryption implementation plans and agency efforts to inventory the sensitive information it holds.

OMB will carefully consider these recommendations to determine whether or not any additional activities in these areas will help to improve the effective implementation and use of encryption products across the Federal government. In particular, we will attempt to leverage existing government wide educational vehicles and forums, such as the CIO Council's Best Practices Committee.

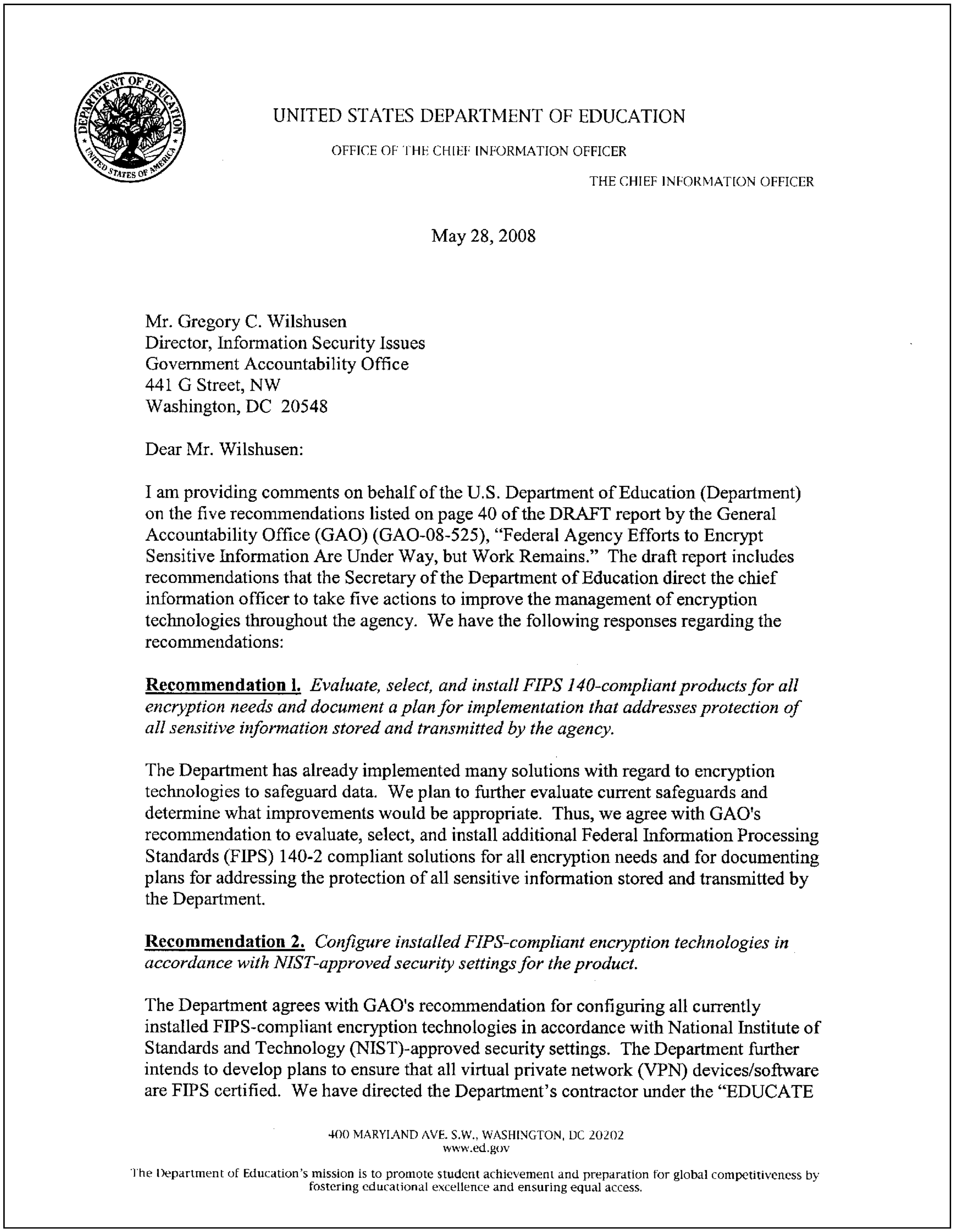
Thank you again for the opportunity to comment on the draft report.

Sincerely,

For

Karen S. Evans
Administrator, Office of E-Government and Information Technology

Appendix VI: Comments from the Department of Education



UNITED STATES DEPARTMENT OF EDUCATION

OFFICE OF THE CHIEF INFORMATION OFFICER

THE CHIEF INFORMATION OFFICER

May 28, 2008

Mr. Gregory C. Wilshusen
Director, Information Security Issues
Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Wilshusen:

I am providing comments on behalf of the U.S. Department of Education (Department) on the five recommendations listed on page 40 of the DRAFT report by the General Accountability Office (GAO) (GAO-08-525), "Federal Agency Efforts to Encrypt Sensitive Information Are Under Way, but Work Remains." The draft report includes recommendations that the Secretary of the Department of Education direct the chief information officer to take five actions to improve the management of encryption technologies throughout the agency. We have the following responses regarding the recommendations:

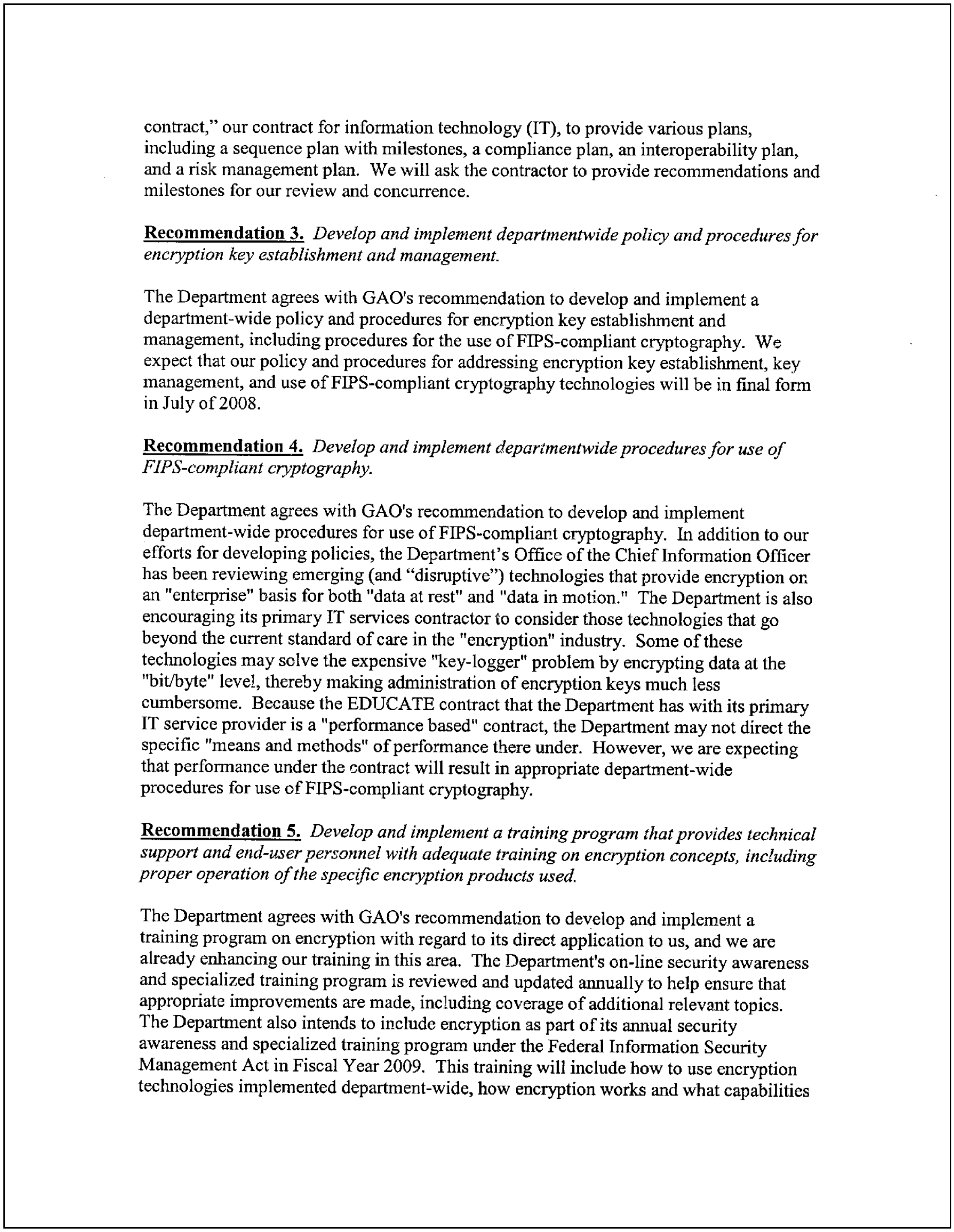
Recommendation l. *Evaluate, select, and install FIPS 140-compliant products for all encryption needs and document a plan for implementation that addresses protection of all sensitive information stored and transmitted by the agency.*

The Department has already implemented many solutions with regard to encryption technologies to safeguard data. We plan to further evaluate current safeguards and determine what improvements would be appropriate. Thus, we agree with GAO's recommendation to evaluate, select, and install additional Federal Information Processing Standards (FIPS) 140-2 compliant solutions for all encryption needs and for documenting plans for addressing the protection of all sensitive information stored and transmitted by the Department.

Recommendation 2. *Configure installed FIPS-compliant encryption technologies in accordance with NIST-approved security settings for the product.*

The Department agrees with GAO's recommendation for configuring all currently installed FIPS-compliant encryption technologies in accordance with National Institute of Standards and Technology (NIST)-approved security settings. The Department further intends to develop plans to ensure that all virtual private network (VPN) devices/software are FIPS certified. We have directed the Department's contractor under the "EDUCATE

The Department of Education's mission is to promote student achievement and preparation for global competitiveness by fostering educational excellence and ensuring equal access.



contract," our contract for information technology (IT), to provide various plans, including a sequence plan with milestones, a compliance plan, an interoperability plan, and a risk management plan. We will ask the contractor to provide recommendations and milestones for our review and concurrence.

Recommendation 3. *Develop and implement departmentwide policy and procedures for encryption key establishment and management.*

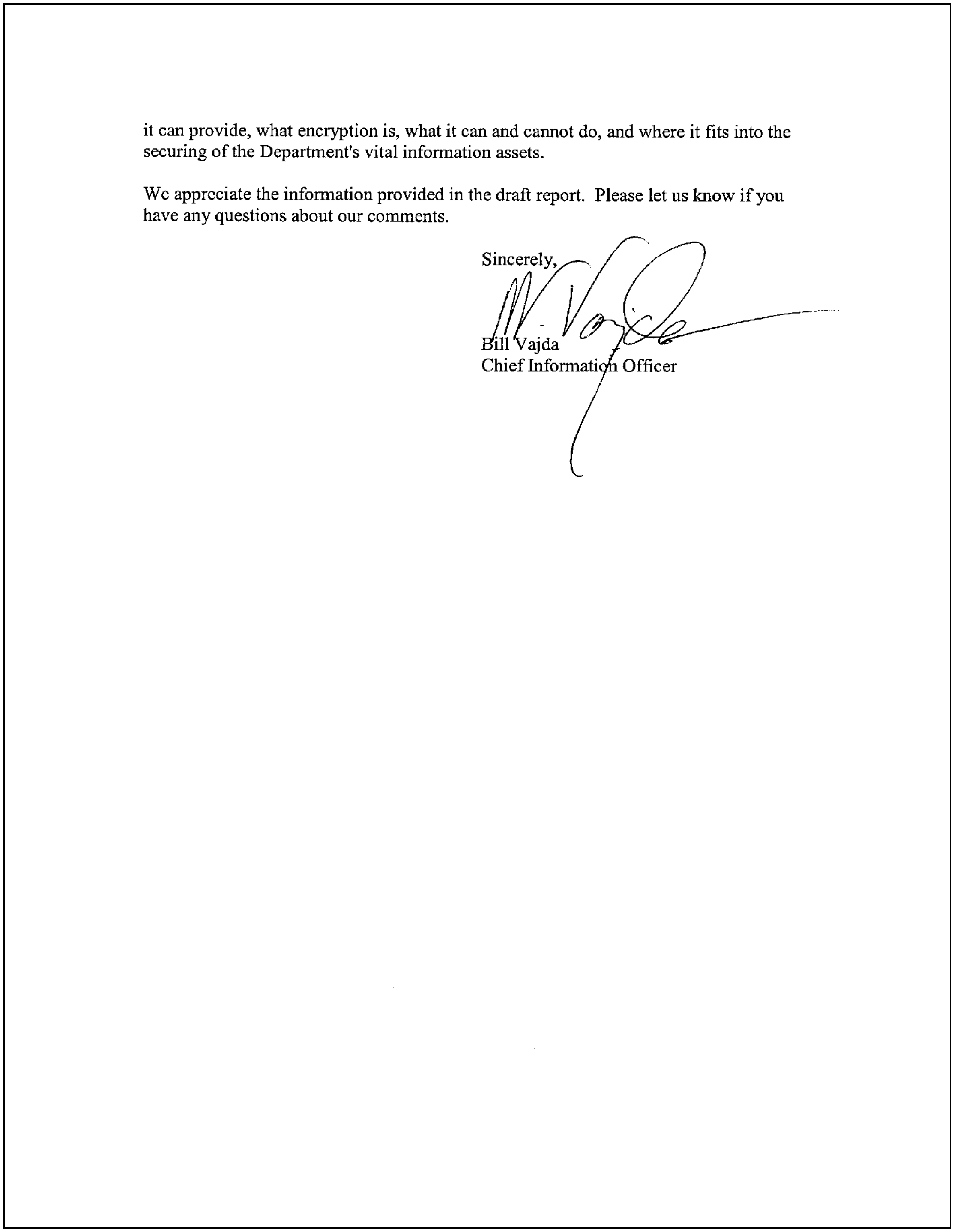
The Department agrees with GAO's recommendation to develop and implement a department-wide policy and procedures for encryption key establishment and management, including procedures for the use of FIPS-compliant cryptography. We expect that our policy and procedures for addressing encryption key establishment, key management, and use of FIPS-compliant cryptography technologies will be in final form in July of 2008.

Recommendation 4. *Develop and implement departmentwide procedures for use of FIPS-compliant cryptography.*

The Department agrees with GAO's recommendation to develop and implement department-wide procedures for use of FIPS-compliant cryptography. In addition to our efforts for developing policies, the Department's Office of the Chief Information Officer has been reviewing emerging (and "disruptive") technologies that provide encryption on an "enterprise" basis for both "data at rest" and "data in motion." The Department is also encouraging its primary IT services contractor to consider those technologies that go beyond the current standard of care in the "encryption" industry. Some of these technologies may solve the expensive "key-logger" problem by encrypting data at the "bit/byte" level, thereby making administration of encryption keys much less cumbersome. Because the EDUCATE contract that the Department has with its primary IT service provider is a "performance based" contract, the Department may not direct the specific "means and methods" of performance there under. However, we are expecting that performance under the contract will result in appropriate department-wide procedures for use of FIPS-compliant cryptography.

Recommendation 5. *Develop and implement a training program that provides technical support and end-user personnel with adequate training on encryption concepts, including proper operation of the specific encryption products used.*

The Department agrees with GAO's recommendation to develop and implement a training program on encryption with regard to its direct application to us, and we are already enhancing our training in this area. The Department's on-line security awareness and specialized training program is reviewed and updated annually to help ensure that appropriate improvements are made, including coverage of additional relevant topics. The Department also intends to include encryption as part of its annual security awareness and specialized training program under the Federal Information Security Management Act in Fiscal Year 2009. This training will include how to use encryption technologies implemented department-wide, how encryption works and what capabilities



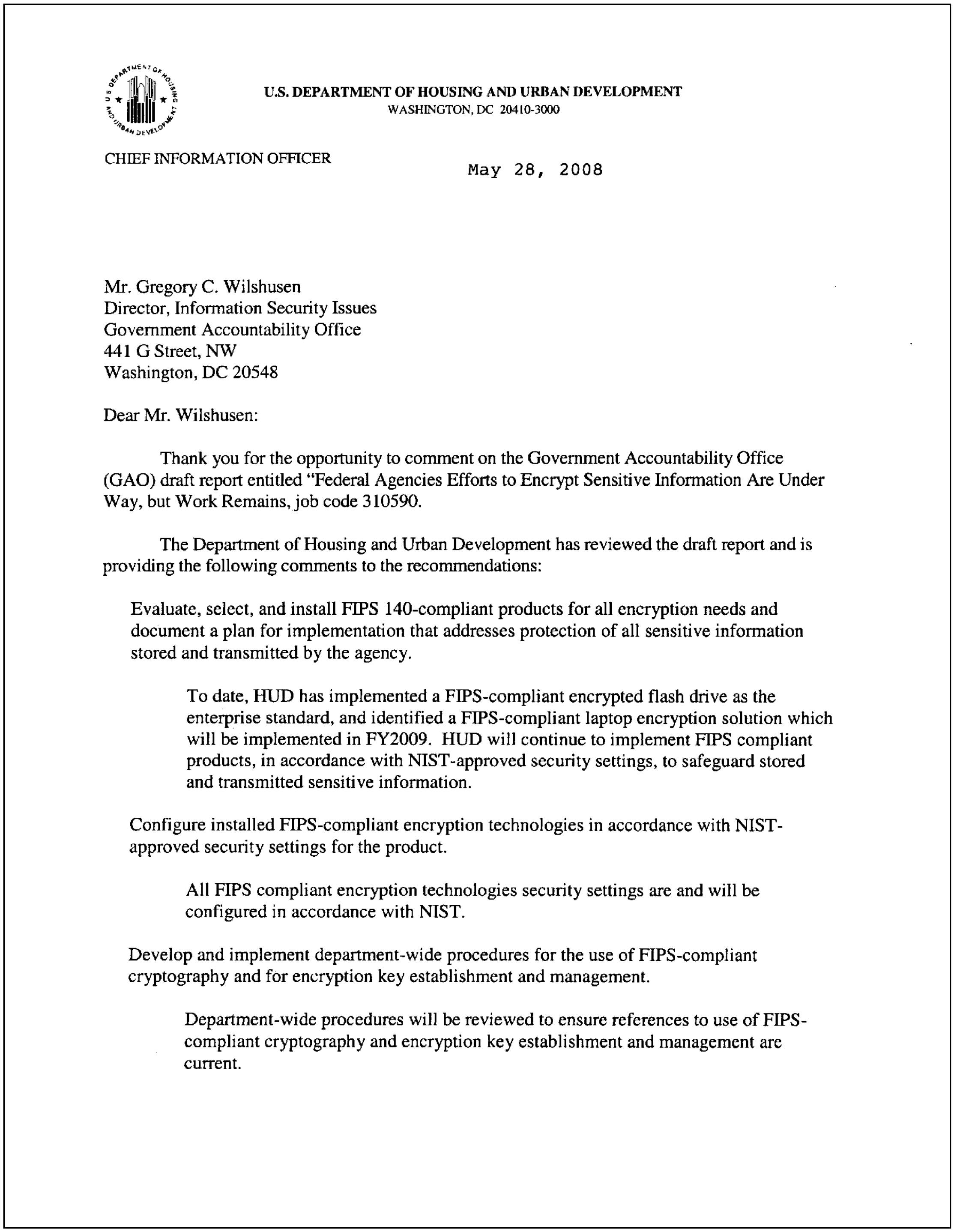
it can provide, what encryption is, what it can and cannot do, and where it fits into the securing of the Department's vital information assets.

We appreciate the information provided in the draft report. Please let us know if you have any questions about our comments.

Sincerely,

Bill Vajda
Chief Information Officer

Appendix VII: Comments from the Department of Housing and Urban Development



U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT
WASHINGTON, DC 20410-3000

CHIEF INFORMATION OFFICER

May 28, 2008

Mr. Gregory C. Wilshusen
Director, Information Security Issues
Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Wilshusen:

Thank you for the opportunity to comment on the Government Accountability Office (GAO) draft report entitled "Federal Agencies Efforts to Encrypt Sensitive Information Are Under Way, but Work Remains, job code 310590.

The Department of Housing and Urban Development has reviewed the draft report and is providing the following comments to the recommendations:

Evaluate, select, and install FIPS 140-compliant products for all encryption needs and document a plan for implementation that addresses protection of all sensitive information stored and transmitted by the agency.

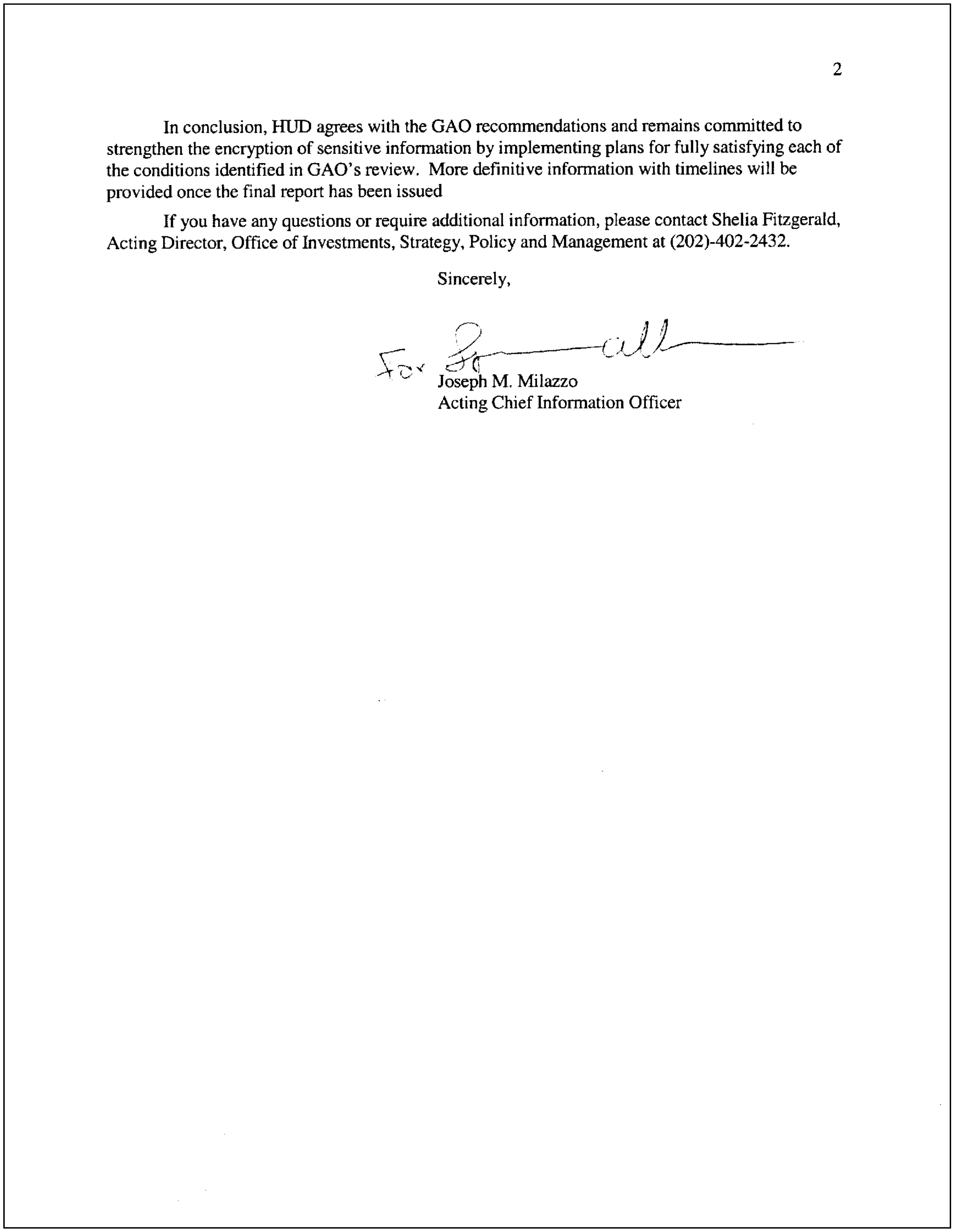
To date, HUD has implemented a FIPS-compliant encrypted flash drive as the enterprise standard, and identified a FIPS-compliant laptop encryption solution which will be implemented in FY2009. HUD will continue to implement FIPS compliant products, in accordance with NIST-approved security settings, to safeguard stored and transmitted sensitive information.

Configure installed FIPS-compliant encryption technologies in accordance with NIST-approved security settings for the product.

All FIPS compliant encryption technologies security settings are and will be configured in accordance with NIST.

Develop and implement department-wide procedures for the use of FIPS-compliant cryptography and for encryption key establishment and management.

Department-wide procedures will be reviewed to ensure references to use of FIPS-compliant cryptography and encryption key establishment and management are current.



In conclusion, HUD agrees with the GAO recommendations and remains committed to strengthen the encryption of sensitive information by implementing plans for fully satisfying each of the conditions identified in GAO's review. More definitive information with timelines will be provided once the final report has been issued

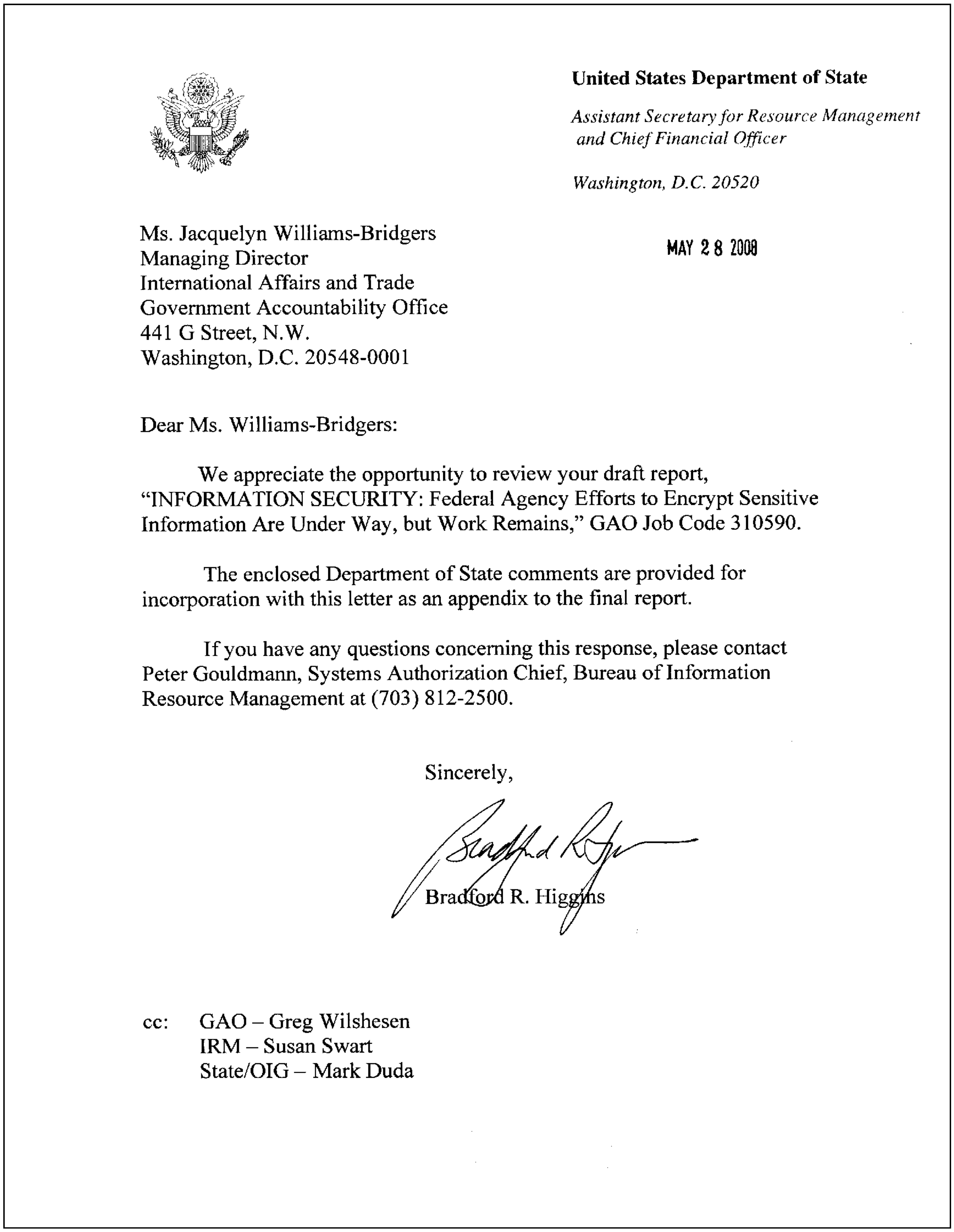
If you have any questions or require additional information, please contact Shelia Fitzgerald, Acting Director, Office of Investments, Strategy, Policy and Management at (202)-402-2432.

Sincerely,

For

Joseph M. Milazzo
Acting Chief Information Officer

Appendix VIII: Comments from the Department of State



United States Department of State

Assistant Secretary for Resource Management
and Chief Financial Officer

Washington, D.C. 20520

MAY 28 2008

Ms. Jacquelyn Williams-Bridgers
Managing Director
International Affairs and Trade
Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548-0001

Dear Ms. Williams-Bridgers:

We appreciate the opportunity to review your draft report, "INFORMATION SECURITY: Federal Agency Efforts to Encrypt Sensitive Information Are Under Way, but Work Remains," GAO Job Code 310590.

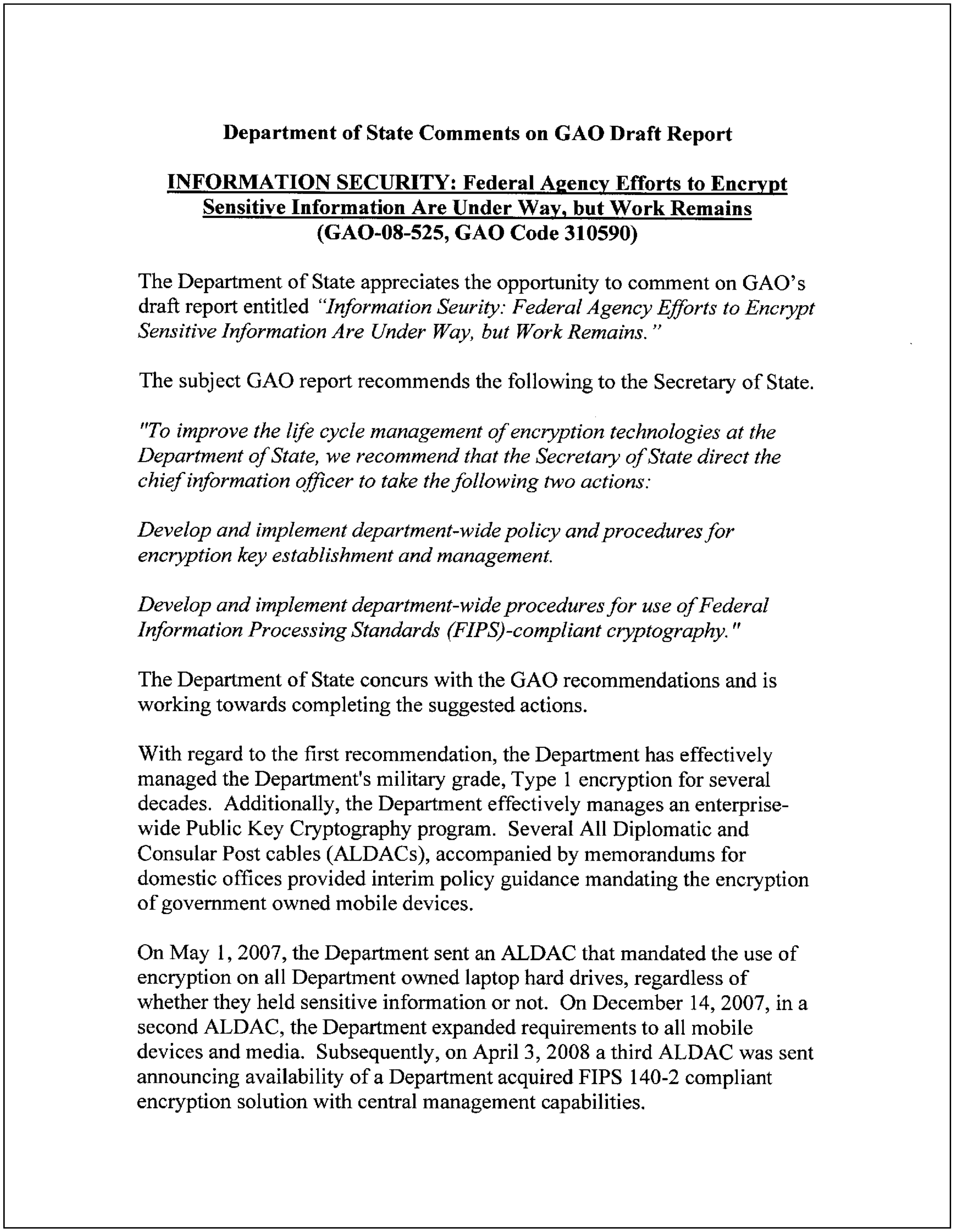
The enclosed Department of State comments are provided for incorporation with this letter as an appendix to the final report.

If you have any questions concerning this response, please contact Peter Gouldmann, Systems Authorization Chief, Bureau of Information Resource Management at (703) 812-2500.

Sincerely,

Bradford R. Higgins

cc: GAO – Greg Wilshesen
IRM – Susan Swart
State/OIG – Mark Duda



Department of State Comments on GAO Draft Report

INFORMATION SECURITY: Federal Agency Efforts to Encrypt Sensitive Information Are Under Way, but Work Remains
(GAO-08-525, GAO Code 310590)

The Department of State appreciates the opportunity to comment on GAO's draft report entitled *"Information Seurity: Federal Agency Efforts to Encrypt Sensitive Information Are Under Way, but Work Remains."*

The subject GAO report recommends the following to the Secretary of State.

"To improve the life cycle management of encryption technologies at the Department of State, we recommend that the Secretary of State direct the chief information officer to take the following two actions:

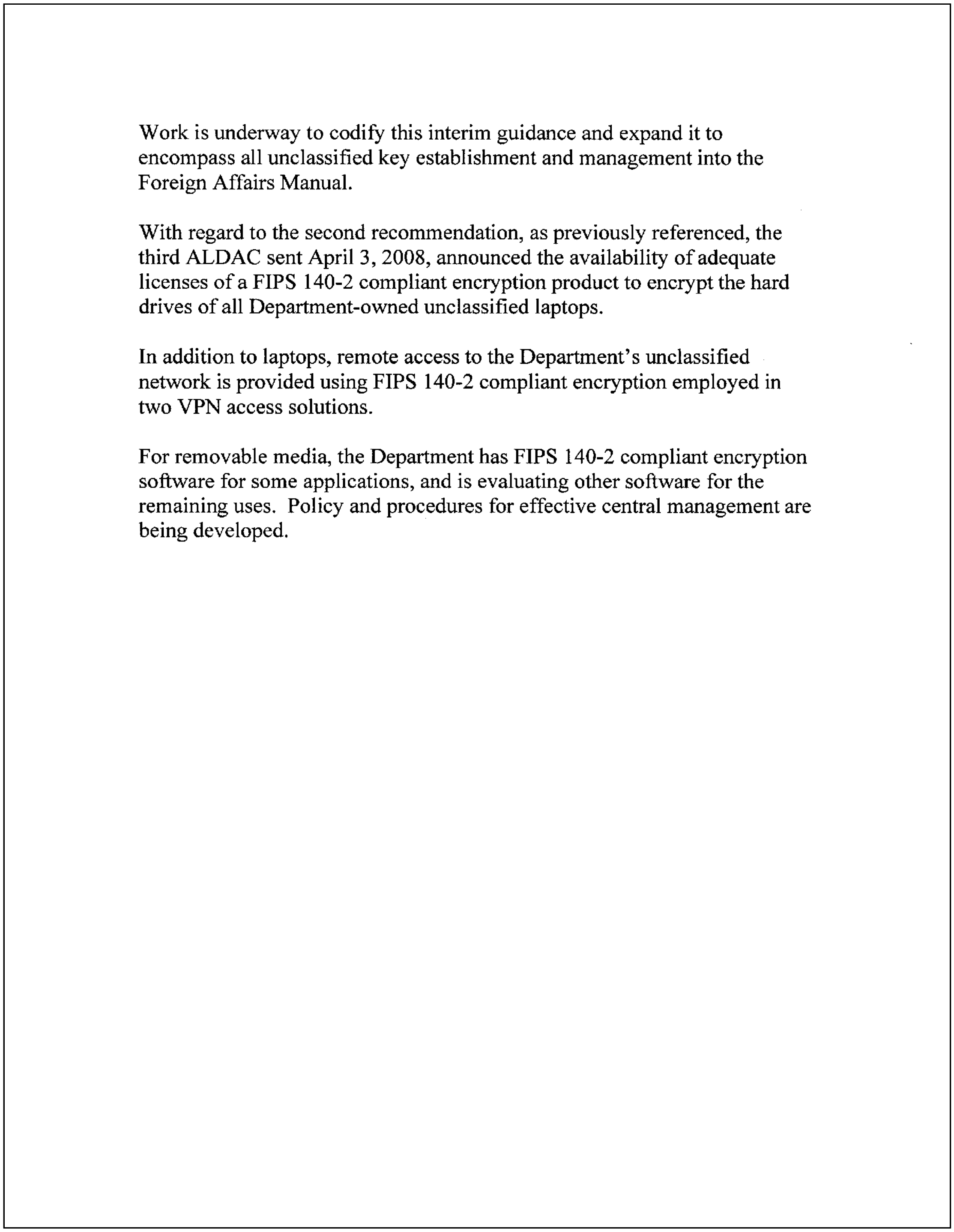
Develop and implement department-wide policy and procedures for encryption key establishment and management.

Develop and implement department-wide procedures for use of Federal Information Processing Standards (FIPS)-compliant cryptography."

The Department of State concurs with the GAO recommendations and is working towards completing the suggested actions.

With regard to the first recommendation, the Department has effectively managed the Department's military grade, Type 1 encryption for several decades. Additionally, the Department effectively manages an enterprise-wide Public Key Cryptography program. Several All Diplomatic and Consular Post cables (ALDACs), accompanied by memorandums for domestic offices provided interim policy guidance mandating the encryption of government owned mobile devices.

On May 1, 2007, the Department sent an ALDAC that mandated the use of encryption on all Department owned laptop hard drives, regardless of whether they held sensitive information or not. On December 14, 2007, in a second ALDAC, the Department expanded requirements to all mobile devices and media. Subsequently, on April 3, 2008 a third ALDAC was sent announcing availability of a Department acquired FIPS 140-2 compliant encryption solution with central management capabilities.



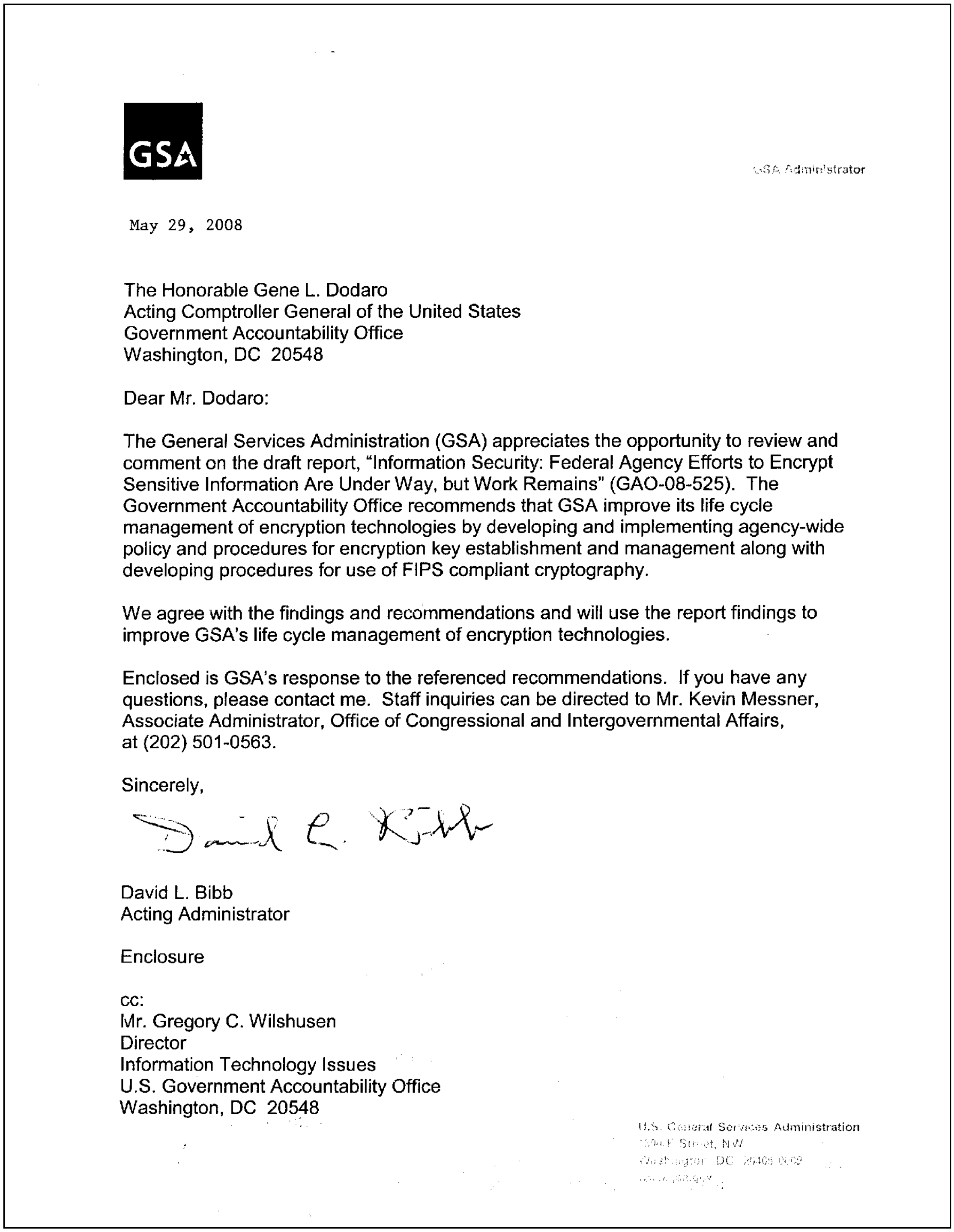
Work is underway to codify this interim guidance and expand it to encompass all unclassified key establishment and management into the Foreign Affairs Manual.

With regard to the second recommendation, as previously referenced, the third ALDAC sent April 3, 2008, announced the availability of adequate licenses of a FIPS 140-2 compliant encryption product to encrypt the hard drives of all Department-owned unclassified laptops.

In addition to laptops, remote access to the Department's unclassified network is provided using FIPS 140-2 compliant encryption employed in two VPN access solutions.

For removable media, the Department has FIPS 140-2 compliant encryption software for some applications, and is evaluating other software for the remaining uses. Policy and procedures for effective central management are being developed.

Appendix IX: Comments from the General Services Administration



GSA

GSA Administrator

May 29, 2008

The Honorable Gene L. Dodaro
Acting Comptroller General of the United States
Government Accountability Office
Washington, DC 20548

Dear Mr. Dodaro:

The General Services Administration (GSA) appreciates the opportunity to review and comment on the draft report, "Information Security: Federal Agency Efforts to Encrypt Sensitive Information Are Under Way, but Work Remains" (GAO-08-525). The Government Accountability Office recommends that GSA improve its life cycle management of encryption technologies by developing and implementing agency-wide policy and procedures for encryption key establishment and management along with developing procedures for use of FIPS compliant cryptography.

We agree with the findings and recommendations and will use the report findings to improve GSA's life cycle management of encryption technologies.

Enclosed is GSA's response to the referenced recommendations. If you have any questions, please contact me. Staff inquiries can be directed to Mr. Kevin Messner, Associate Administrator, Office of Congressional and Intergovernmental Affairs, at (202) 501-0563.

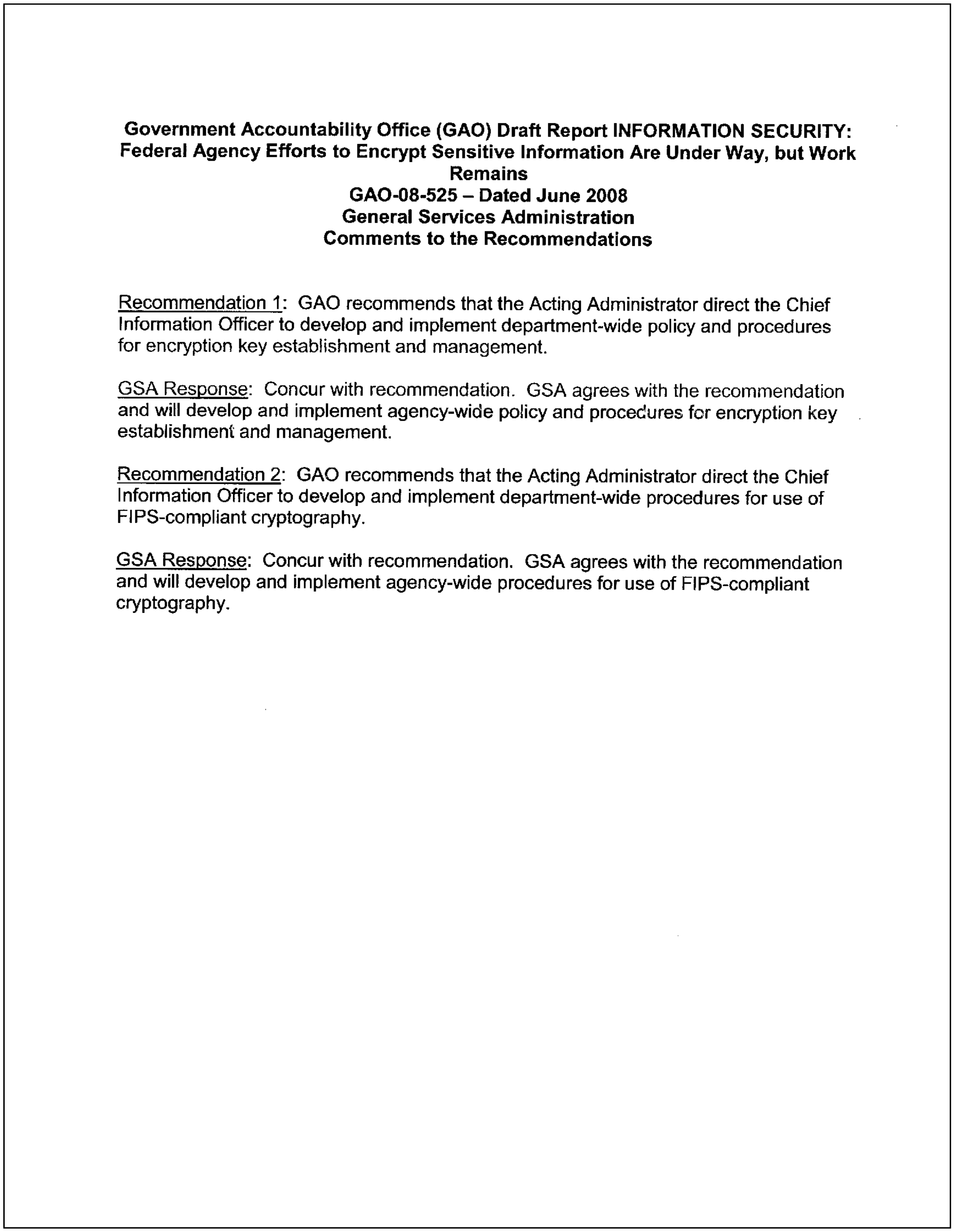
Sincerely,

David L. Bibb
Acting Administrator

Enclosure

cc:
Mr. Gregory C. Wilshusen
Director
Information Technology Issues
U.S. Government Accountability Office
Washington, DC 20548

U.S. General Services Administration
1800 F Street, NW
Washington, DC 20405-0002
www.gsa.gov



Government Accountability Office (GAO) Draft Report INFORMATION SECURITY: Federal Agency Efforts to Encrypt Sensitive Information Are Under Way, but Work Remains
GAO-08-525 – Dated June 2008
General Services Administration
Comments to the Recommendations

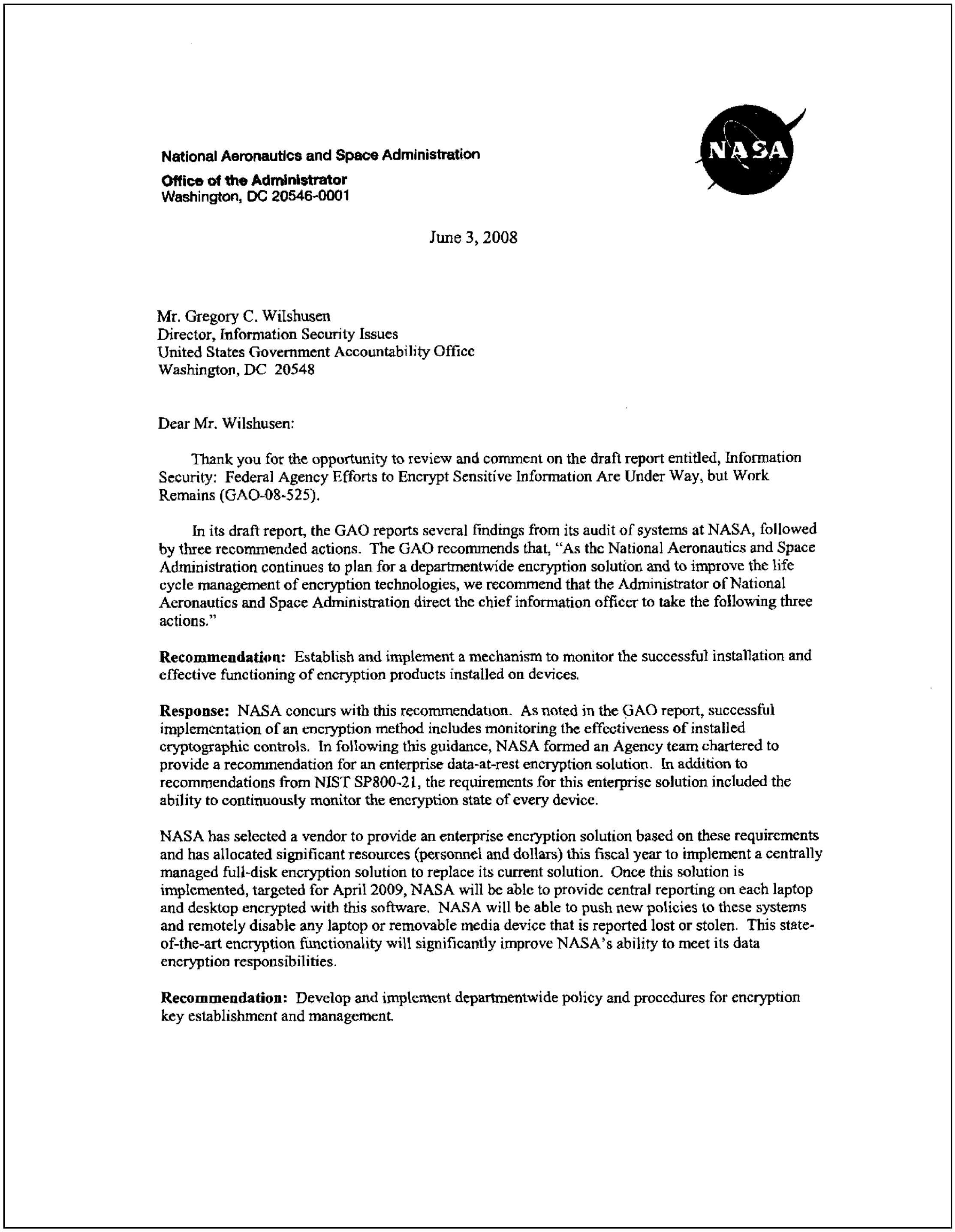
Recommendation 1: GAO recommends that the Acting Administrator direct the Chief Information Officer to develop and implement department-wide policy and procedures for encryption key establishment and management.

GSA Response: Concur with recommendation. GSA agrees with the recommendation and will develop and implement agency-wide policy and procedures for encryption key establishment and management.

Recommendation 2: GAO recommends that the Acting Administrator direct the Chief Information Officer to develop and implement department-wide procedures for use of FIPS-compliant cryptography.

GSA Response: Concur with recommendation. GSA agrees with the recommendation and will develop and implement agency-wide procedures for use of FIPS-compliant cryptography.

Appendix X: Comments from the National Aeronautics and Space Administration



National Aeronautics and Space Administration

Office of the Administrator
Washington, DC 20546-0001

June 3, 2008

Mr. Gregory C. Wilshusen
Director, Information Security Issues
United States Government Accountability Office
Washington, DC 20548

Dear Mr. Wilshusen:

Thank you for the opportunity to review and comment on the draft report entitled, Information Security: Federal Agency Efforts to Encrypt Sensitive Information Are Under Way, but Work Remains (GAO-08-525).

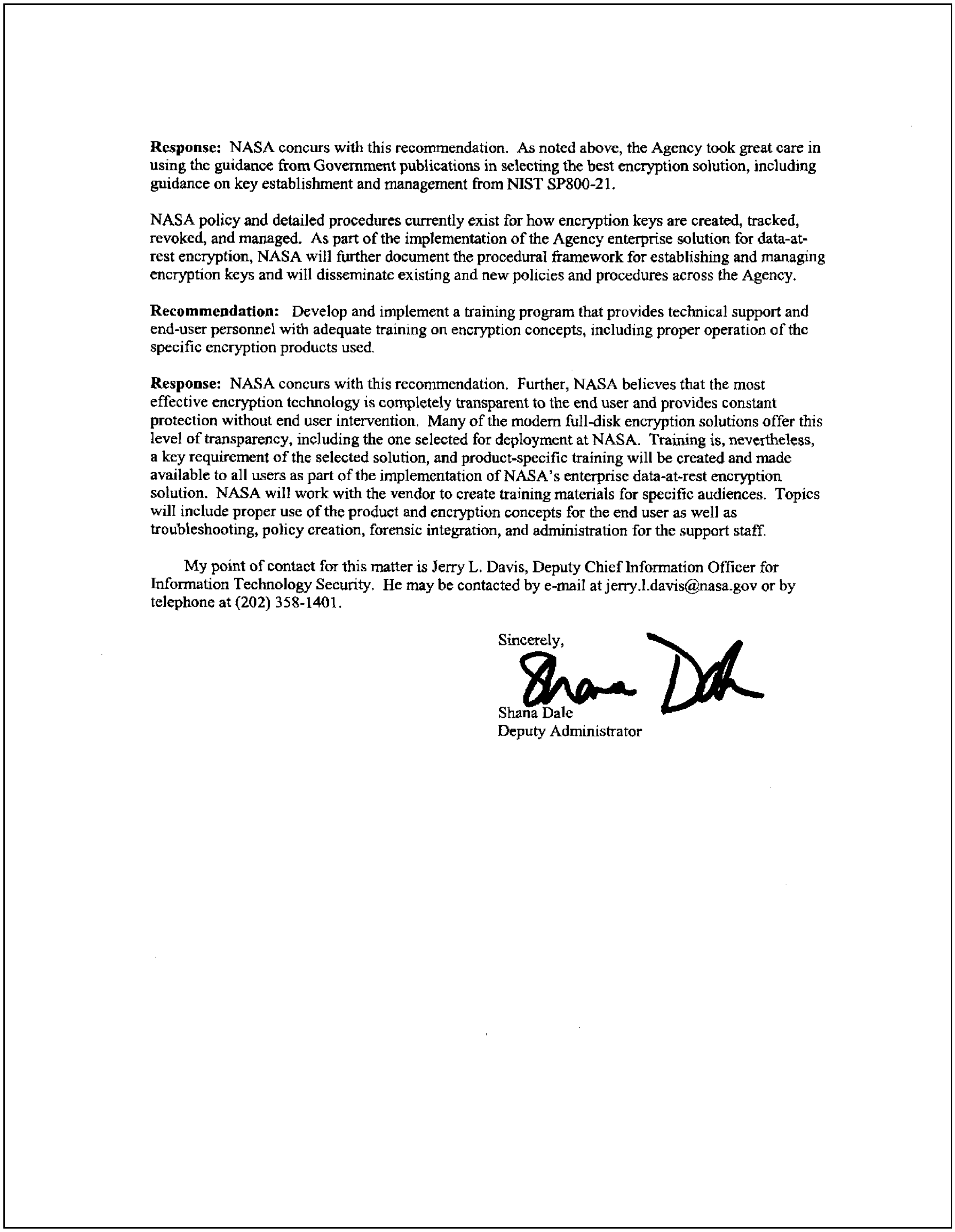
In its draft report, the GAO reports several findings from its audit of systems at NASA, followed by three recommended actions. The GAO recommends that, "As the National Aeronautics and Space Administration continues to plan for a departmentwide encryption solution and to improve the life cycle management of encryption technologies, we recommend that the Administrator of National Aeronautics and Space Administration direct the chief information officer to take the following three actions."

Recommendation: Establish and implement a mechanism to monitor the successful installation and effective functioning of encryption products installed on devices.

Response: NASA concurs with this recommendation. As noted in the GAO report, successful implementation of an encryption method includes monitoring the effectiveness of installed cryptographic controls. In following this guidance, NASA formed an Agency team chartered to provide a recommendation for an enterprise data-at-rest encryption solution. In addition to recommendations from NIST SP800-21, the requirements for this enterprise solution included the ability to continuously monitor the encryption state of every device.

NASA has selected a vendor to provide an enterprise encryption solution based on these requirements and has allocated significant resources (personnel and dollars) this fiscal year to implement a centrally managed full-disk encryption solution to replace its current solution. Once this solution is implemented, targeted for April 2009, NASA will be able to provide central reporting on each laptop and desktop encrypted with this software. NASA will be able to push new policies to these systems and remotely disable any laptop or removable media device that is reported lost or stolen. This state-of-the-art encryption functionality will significantly improve NASA's ability to meet its data encryption responsibilities.

Recommendation: Develop and implement departmentwide policy and procedures for encryption key establishment and management.



Response: NASA concurs with this recommendation. As noted above, the Agency took great care in using the guidance from Government publications in selecting the best encryption solution, including guidance on key establishment and management from NIST SP800-21.

NASA policy and detailed procedures currently exist for how encryption keys are created, tracked, revoked, and managed. As part of the implementation of the Agency enterprise solution for data-at-rest encryption, NASA will further document the procedural framework for establishing and managing encryption keys and will disseminate existing and new policies and procedures across the Agency.

Recommendation: Develop and implement a training program that provides technical support and end-user personnel with adequate training on encryption concepts, including proper operation of the specific encryption products used.

Response: NASA concurs with this recommendation. Further, NASA believes that the most effective encryption technology is completely transparent to the end user and provides constant protection without end user intervention. Many of the modern full-disk encryption solutions offer this level of transparency, including the one selected for deployment at NASA. Training is, nevertheless, a key requirement of the selected solution, and product-specific training will be created and made available to all users as part of the implementation of NASA's enterprise data-at-rest encryption solution. NASA will work with the vendor to create training materials for specific audiences. Topics will include proper use of the product and encryption concepts for the end user as well as troubleshooting, policy creation, forensic integration, and administration for the support staff.

My point of contact for this matter is Jerry L. Davis, Deputy Chief Information Officer for Information Technology Security. He may be contacted by e-mail at jerry.l.davis@nasa.gov or by telephone at (202) 358-1401.

Sincerely,

Shana Dale

Shana Dale
Deputy Administrator

Appendix XI: GAO Contact and Staff Acknowledgments

GAO Contact

Gregory C. Wilshusen, (202) 512-6244, wilshuseng@gao.gov

Staff Acknowledgments

In addition to the individual named above, Nancy DeFrancesco (Assistant Director), James Ashley, Debra Conner; Season Dietrich, Neil Doherty, Nancy Glover, Joel Grossman, Ethan Iczkovitz, Stanley J. Kostyla, Lowell Labaro, Rebecca Lapaze, Anjalique Lawrence, Harold Lewis, Lee McCracken, and Tammi L. Nguyen made key contributions to this report.

Glossary

Access Control

Process of determining the permissible activities of users and authorizing or prohibiting activities by each user.

Authentication

Process of confirming an asserted identity with a specified or understood level of confidence.

Authorization

Granting the appropriate access privileges to authenticated users.

Card Management System

A system that manages life cycle maintenance tasks associated with the credentials, such as unlocking the personal identity verification cards during issuance or updating a personal identification number or digital certificate on the card.

Certificate

A digital representation of information that (1) identifies the authority issuing the certificate; (2) names or identifies the person, process, or equipment using the certificate; (3) contains the user's public key; (4) identifies the certificate's operational period; and (5) is digitally signed by the certificate authority issuing it. A certificate is the means by which a user is linked—or bound—to a public key.

Ciphertext

Data in an encrypted form.

Container

The file used by a virtual disk encryption technology to encompass and protect other files.

Credential

An object, such as a smart card, that identifies an individual as an official representative of, for example, a government agency.

Digital Signature

The result of the transformation of a message by means of a cryptographic system using digital keys, so that a relying party can determine (1) whether the transformation was created using the private key that corresponds to the public key in the signer's digital certificate and (2) whether the message has been altered since the transformation was made. Digital signatures may also be attached to other electronic information and programs so that the integrity of the information and programs may be verified at a later time.

Electronic Credentials

The electronic equivalent of a traditional paper-based credential—a document that vouches for an individual's identity.

End-to-End Encryption

The encryption of information at its origin and decryption at its intended destination without any intermediate decryption.

File

A collection of information that is logically grouped into a single entity and referenced by a unique name, such as a file name.

Folder

An organizational structure used to group files.

Full Disk Encryption

The process of encrypting all the data on the hard drive used to boot a computer, including the computer's operating system, that permits access to the data only after successful authentication with the full disk encryption product.

Hardware Based Encryption

Encryption that is normally performed by dedicated hardware in the client/host system.

Identification

The process of determining to what identity a particular individual corresponds.

Key

A value used to control cryptographic operations, such as decryption, encryption, signature generation, or signature verification.

Malware

A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim.

Master Boot Record

A computer's master boot record is a reserved sector on its bootable media that determines which software (e.g., operating system, utility) will be executed when the computer boots from the media.

Operating System

The program that, after being initially loaded into the computer by a boot program, manages all the other programs in a computer. Examples of operating systems include Microsoft Windows, MacOS, and Linux. The other programs are called applications or application programs. The application programs make use of the operating system by making a request for service through a defined application program interface. In addition, users can interact directly with the operating system through a user interface such as a command language or a graphical user interface.

Private Key

The secret part of an asymmetric key pair that is typically used to digitally sign or decrypt data.

Public Key

The public part of an asymmetric key pair that is typically used to verify signatures or encrypt data.

Public Key Infrastructure

A system of hardware, software, policies, and people that, when fully and properly implemented, can provide a suite of information security assurances—including confidentiality, data integrity, authentication, and nonrepudiation—that are important in protecting sensitive communications and transactions.

Risk

The expectation of loss expressed as the probability that a threat will exploit a vulnerability with a harmful result.

Senstitive Information

Any information that an agency has determined requires some degree of heightened protection from unauthorized access, use, disclosure, disruption, modification, or destruction because of the nature of the information, e.g., personal information required to be protected by the Privacy Act of 1974, proprietary commercial information, information critical to agency program activities, and information that has or may be determined to be exempt from public release under the Freedom of Information Act.

Standard

A statement published on a given topic by organizations such as the National Institute of Standards and Technology, the Institute of Electrical and Electronics Engineers, the International Organization for Standardization, and others specifying characteristics—usually measurable ones—that must be satisfied to comply with the standard.

Trusted Platform Module Chip

A tamper-resistant integrated circuit built into some computer motherboards that can perform cryptographic operations (including key generation) and protect small amounts of sensitive information such as passwords and cryptographic keys.

Virtual Disk Encryption

The process of encrypting a container, which can hold many files and folders, and of permitting access to the data within the container only after proper authentication is provided. In this case, the container is typically mounted as a virtual disk; it appears to the user as a logical disk drive.

Virtual Private Network

A virtual private network is a logical network that is established, at the application layer of the open systems interconnection model, over an existing physical network and typically does not include every node present on the physical network.

(310590)

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "E-mail Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, DC 20548

To order by Phone:	Voice:	(202) 512-6000
	TDD:	(202) 512-2537
	Fax:	(202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548