

A photograph of a stone wall with crenellations, likely part of a historical fortification or castle. The wall is made of rough-hewn stones and has several square towers along the top. A small arched opening is visible in the wall. The background shows a clear blue sky and some greenery.

Sensitive Data Classification and Protection

Overcoming the Challenges to Classify and Protect
Sensitive Data at Federal Government Agencies

Background

Sensitive Data within Federal Government Information Systems

All U.S federal government agencies are supported by computer information systems. These systems enable agencies to carry out their missions and account for their resources. With computer networks and information systems comes security risk. The risks range from unauthorized access which can lead to lost or stolen data or to attacks which disrupt or limit business processes.

Of particular concern is the protection of sensitive information maintained by Federal agencies. Depending on the mission of the agency, sensitive data can range from information pertaining to criminal investigations, information associated with managing financial resources or data regarding emergency preparedness. If this type of sensitive information were inappropriately disclosed, browsed, or copied for improper or criminal purposes, it could be used to disrupt critical government operations such as those supporting homeland security, financial services, public safety or emergency services. Sensitive data also includes information under the due care of Federal agencies that is sensitive to individuals or corporations. Examples of this type of data include taxpayer data, Social Security records, medical records, proprietary information and business financial information. Individual's privacy, personal freedoms or finances along with confidentiality of business information could be severely impacted if security is breached or data is improperly disclosed. Security incidents involving this form of sensitive data can undermine the agency resulting in diminished confidence and impact on current operations.



Data Classification and Implications on Information Security

National Security Information

[Executive Order 12958](#) prescribes a uniform system for classifying, safeguarding, and declassifying national security information. Since its issue in 1995, organizations of the Federal government have implemented its processes. Over that time, the order has been amended to address national interests. Agencies that process national security information typically have well-established policy, processes and organizations to support physical, industrial, information, communication and cyber security associated with national security information and systems.

Sensitive But Unclassified (SBU)

The term "Sensitive But Unclassified" (SBU) originated with the Computer Security Act of 1987. It defined SBU as "any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, United States Code (USC) (the Privacy Act) but which has not been specifically authorized under criteria established by an executive order or an act of Congress to be kept secret in the interest of national defense or foreign policy." The Computer Security Act of 1987 was superseded by FISMA in 2002, however FISMA did not redefine the term SBU.

Congress has enacted laws which provided agencies responsibilities for certain types of sensitive information. The following laws, orders and directives identify forms of sensitive information:

There have already been more data breaches reported this year in the US than were reported in all of 2007.

Businesses, government agencies and universities have reported 449 data breaches so far this year.

- Identity Theft Resource Center

- Freedom of Information Act of 1966, as Amended (5 USC 552)
- Homeland Security Act of 2002 (Public Law 107-296, 116 Stat. 2135)
- Health Insurance Portability and Accountability Act (HIPAA) Security Regulations 45 CFR Parts 160, 162, and 164
- Family Educational Government Rights and Privacy Act (FERPA) Regulations CFR Part 99
- Foreign Assistance Act of 1961, as amended;
- Privacy Act of 1974;
- Freedom of Information Act;
- Computer Security Act of 1987;
- Trade Secrets Act;
- Federal Managers Financial Integrity Act of 1982;
- Department of Health and Human Government Services (HHS) Title 45 CFR Part 46 Protection of Human Subjects; and
- Federal Acquisition Regulations (FAR)

Federal agencies have recognized that they must properly protect and handle government information to prevent the data from compromising U.S. national security as well as personal privacy. Since agencies handle many different forms of “sensitive” information, that gave way to the creation of numerous new subcategories for marking and managing sensitive information¹. Many agencies use Sensitive But Unclassified (SBU) but have unique rules regarding its labeling, handling and protection. The Department of Energy uses Official Use Only (OUO) while the Drug Enforcement Administration uses DEA Sensitive. Other law enforcement organizations use the term Law Enforcement Sensitive (LES) while the Department of Homeland Security uses the term Security Sensitive Information (SSI). In all cases the designations refer to unclassified, sensitive information that is or may be exempt from public release under the Freedom of Information Act.

This evidence demonstrates lack of national guidance or additional specificity that creates confusion and difficulty within the government on how to handle or share sensitive information. Additionally, the lack of national standards creates a barrier to the implementation of automated solutions due to lack of standards and inability to mass market products without customization at each agency.

Privacy Act, E-Government Act and Personally Identifiable Information

The Privacy Act of 1974 established safeguards for privacy of records of citizens through the creation of procedural and substantive rights to personal data. The Act requires government agencies to provide an individual with access to records that are maintained by the agency that contain the personal information on the requesting individual. The Act further requires agencies to follow principles, called “fair information practices,” when gathering and handling personal data. The Privacy Act places restrictions on how agencies can share an individual's data with other people and agencies.

Section 208 of the E-Government Act of 2002 (Public Law 107-347, 44 U.S.C.) directed OMB to issue guidance to agencies for implementing the privacy provisions of the E-Government Act. The E-Government Act requires federal agencies to conduct Privacy Impact Assessments (PIA) before developing or procuring information technology or initiating any new collections of Personally Identifiable

The Office of Management and Budget issued a series of guidance memos that specify directs agencies to minimize sensitive data held, increase its protection and speed incident response:

- *A breach notification policy (Attachment 3 of OMB Memo 07-16)*
- *An implementation plan to eliminate unnecessary use of Social Security Numbers (SSN) (Attachment 1 of OMB Memo 07-16)*
- *An implementation plan and progress update on review and reduction of holdings of personally identifiable information (PII) (Attachment 1 of OMB Memo 07-16)*
- *A policy outlining rules of behavior and identifying consequences and corrective actions available for failure to follow these rules (Attachment 4 of OMB M-07-16)*
- *Additionally, OMB requires CIOs to report and certify on their progress annually in its agencies FISMA report.*

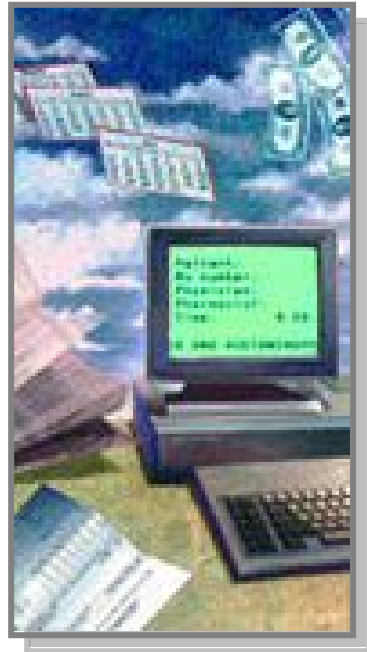
- OMB

¹ Laws and Regulations Governing the Protection of SBU Information, Federal Research Division, Library of Congress, 2004

Information (PII)². When information in identifiable form is gathered by any system or application, then the requirement to conduct a PIA applies regardless of the individuals involved whether they are members of the public, government personnel, or government contractors and consultants.

The Office of Management and Budget issued memo [M-06-16 "Protection of Sensitive Agency Information"](#) which provided additional guidance to agencies regarding protection of Personally Identifiable Information (PII). This memo required all federal agencies to:

- Encrypt all data on mobile computers/devices which carry agency data unless the data is determined to be non-sensitive. This spans PDAs, laptops, USB storage devices, and backup media;
- Allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access;
- Use a "time-out" function for remote access and mobile devices requiring user re-authentication after 30 minutes inactivity; and
- Log all computer-readable data extracts from databases holding sensitive information and verify each extract including sensitive data has been erased within 90 days or its use is still required.



For Official Use Only

For Official Use Only (FOUO) is a designation used by Federal agencies to identify information or material which, although unclassified, may not be appropriate for public release. There is no national policy governing use of the For Official Use Only designation. DoD Directive 5400.7 defines For Official Use Only information as "unclassified information that may be exempt from mandatory release to the public under the Freedom of Information Act (FOIA)." The policy is implemented by DoD Regulation 5400.7-R and 5200.1-R.

The fact that information is marked FOUO does not mean it is automatically exempt from public release under FOIA. If a request for the information is received, it must be reviewed to see if it meets the FOIA dual test: (1) It fits into one of the nine FOIA exemption categories, and (2) There is a legitimate government purpose served by withholding the information. On the other hand, the absence of the FOUO or other marking does not automatically mean the information must be released in response to a FOIA request.

Controlled Unclassified Information (CUI)

To harmonize standards for handling sensitive documents across the government, the Whitehouse undertook an effort to study the problem. The result was the development of a new framework for managing all unclassified information. On May 9, 2008, the President of the United States issued a Memorandum for the heads of all

"Controlled Unclassified Information" is now the categorical designation that refers to unclassified information that is:

- *pertinent to the national interests of the United States or to the important interests of entities outside the Federal Government, and*
- *under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination.*

- Whitehouse memo

² Information in identifiable form is defined in Section 208(d) of the e-Government Act as "any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means." Information "permitting the physical or online contacting of a specific individual" (see section 208(b)(1)(A)(ii)(II)) is the same as "information in identifiable form."

executive departments and agencies³. The [Designation and Sharing of Controlled Unclassified Information \(CUI\)](#) adopts, defines, and institutes "Controlled Unclassified Information" (CUI) as the single, categorical designation henceforth throughout the executive branch for all information within the scope of that definition, which includes most information heretofore referred to as "Sensitive But Unclassified" (SBU) the Information Sharing Environment (ISE). The purpose of the memo is to standardize practices and thereby improve the sharing of information, not to classify or declassify new or additional information by establishing a corresponding new CUI Framework for designating, marking, safeguarding, and disseminating information designated as CUI.

This Executive Order and the designation CUI replaces the use of "Sensitive But Unclassified" (SBU).

Infrastructure protection agreements not fully accommodated under the CUI Framework (and its associated markings, safeguarding requirements, and dissemination limitations) are permitted exceptions to this CUI Framework. Infrastructure protection exceptions include and apply to information governed by or subject to the following regulations:

- 6 CFR Pt. 29 – PCII (Protected Critical Infrastructure Information);
- 49 CFR Pts. 15 (Department of Transportation) & 1520 (Department of Homeland Security/Transportation Security Administration) – SSI (Sensitive Security Information);
- 6 CFR Pt. 27 – CVI (Chemical Vulnerability Information); and
- 10 CFR Pt. 73 – SGI (Safeguards Information).

On May 22, 2008 the National Archives and Records Administration (NARA) published its initial response⁴ to the Whitehouse memo which laid out the responsibilities of Director of the CUI Office at NARA. Subsequently, the Director issued a memo on June 27 which provided initial implementation guidance to agencies. NARA, in conjunction with the CUI Council, is currently working to issue detailed implementation guidance to agencies. Once issued, agencies will need to adjust internal policies and procedures to incorporate and transition to the use of the new CUI framework.

Challenges of Federal Agencies

A key element in common across all of these requirements is the need for organizations to ensure that controls are operating within predictable boundaries and within acceptable risk and compliance expectations. The General Accounting Office (GAO) found⁵ that numerous Federal agencies have recently experienced security incidents that put sensitive data at risk. Personally identifiable information of millions of Americans has been lost, stolen, or improperly disclosed, thereby exposing those individuals to loss of privacy, identity theft, and financial crimes. Almost all of the major federal agencies had weaknesses in one or more areas of information security



³ "Departments and Agencies" means executive agencies as defined in section 105 of title 5, United States Code; the United States Postal Service; but not the Government Accountability Office.

⁴ <http://www.archives.gov/press/press-releases/2008/nr08-107.html>

⁵ GAO "Information Security - Agencies Report Progress, but Sensitive Data Remain at Risk", GAO-07-935T, June 2007

controls as determined by GAO. Agency heads, Chief Information Officers and Chief Information Security Officers face many challenges to ensure they are effectively protecting information and complying with applicable Federal, industry-specific and agency-specific security and privacy policies.

Federal government Chief Information Officers (CIO) and Chief Information Security Officers (CISOs) are charged with increased responsibility for protecting information. They face a daunting task frequently complicated by siloed security management, monitoring, measurement, and auditing environments. Threats are increasing complex and more targeted which further increases the burden on IT operations. Adding to these burdens and complexity is the fact that the President, Congress and OMB are rapidly enacting new laws and policies that require agencies to implement additional security safeguards, assert more control, and provide detailed metrics to measure performance and demonstrate compliance. Often times, these additional security safeguards and the associated reporting are not funded.

Agency Chief Information Officers, IT and cyber security professionals must address the challenges of security and information assurance while providing their customers and users with data:

- *When it is needed*
- *Where it is needed; and*
- *How it is needed*

Addressing Common Security Risks in Federal Agencies

The Identify Theft Task Force recently reported that there are a series of common risks found in Federal agencies that impede adequate protection of sensitive information are:

- Security and privacy training is inadequate and poorly aligned with the different roles and responsibilities of various personnel.
- Contracts and data sharing agreements lacking security
- Information inventories inaccurately described
- Information is not appropriately scheduled, archived, or destroyed
- Suspicious activities and incidents are not identified and reported in a timely manner.
- Audit trails not appropriately created or reviewed.
- Inadequate physical security controls for information
- Inadequate security control implementation
- Information processed remotely not properly controlled and protected
- Agencies acquire information technology and information security products without incorporating appropriate security and privacy standards and guidelines.

Share Sensitive Information Internally and Externally

All organizations need to share information or provide data to partners to support business processes or achieve missions. For agencies of the Federal government the need to share is driven by multiple operational and mission needs:

- Sharing and collaboration between different groups of the same organization
- Sharing between different defense, law enforcement and intelligence organizations Exchanging data based on Communities of Interest (COI) or coalitions of international partners



- Sharing of data with contractors based on project requirements
- Providing data necessary for outsourced business operations or IT services performed by other federal agencies or contractors

Agencies are typically confronted with one or more of the following challenges when sharing data:

- Inability to limit access control once shared beyond broad connection agreements or Memorandums of Understanding
- Limited ability to control copying or printing content thereby impacting ability to track extracts or printed copies
- Inability to revoke or change access when relationship changes, business need eliminated or contract ends
- Unable to determine when sensitive data has been accessed without authorization which impacts ability to respond to incidents, assess damage and communicate with effected personnel or organizations

Identify, Categorize, Protect and Audit Sensitive Data

Data are some of the most valuable assets any organization possesses or produces. Determining what constitutes appropriate protection is driven by the legal, management, financial and operational requirements required of your agency based on its mission. Protecting data assets while supporting government missions that require information sharing, collaboration, distributed processing and a mobile workforce can be a difficult balancing act. One of the most important steps in protecting data appropriately is to determine the classification for the data used by your agency. Once achieved, organizations can then establish the criticality and minimum security controls for information systems which process, store or transmit this data.

Agencies must determine the applicable guidance for marking and protecting “sensitive” information and then consistently implement this guidance within their agency. This involves developing internal policy and procedures which incorporate the applicable national policy. The personnel with responsibility and authority for designation must be provided education and training to ensure effective execution. Organization-wide IT security awareness must be updated or augmented to communicate policy and ensure all personnel are aware of their responsibilities to ensure the information is properly protected.

FIPS PUB 199⁶ and NIST SP 800-60 provide guidance to categorize information and information systems. These guides recommend a security categorization process for information and information systems and describe a methodology for identifying types of information consistent across the Federal government. If implemented properly, this guidance should identify the information types and the recommended associated security impact levels. However, frequently key information types are missed or the individuals performing the assessment are not aware of the applicable security and privacy policies and requirements which apply to the information contained in the system.



⁶ FIPS PUB 199 defines “information type” as a specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or, in some instances, by a specific law, Executive Order, directive, policy, or regulation.

Many organizations have formal access policies and processes that govern how and when sensitive data is accessed, but lack practical and cost-effective solutions for detecting or blocking activities that fall outside these policies.

Overcome these Challenges

Protecting sensitive information and digital assets is a complex challenge. Unfortunately, the threats to this information and assets continues to grow, are becoming more targeted and sophisticated. At the same time, Agencies are under constant pressure to deliver services more rapidly over a wider array of networks, devices and boundaries. The combination of increasing threats and vulnerabilities together with the demand for ubiquitous access to information and services increases the risk of security breaches and exposures.

Our approach and solutions address the information security challenges faced by many agencies and can be adapted to the unique needs of your agency. We tailor our approach and solutions based on your organizational structure, the data your organization processes and the current level of maturity of your information security program.

Discover, Inventory and Classify Systems and Sensitive Data

Asset Discovery / Network Mapping of your network to discover and categorize all assets. Map the assets to both physical and logical associations (such as FISMA system inventory) to associate security impact levels to assets (FIPS PUB 199 and NIST SP 800-60). Continuously monitor for changes.

- *Agent-less – no need to install software or agents on your IT assets. Scanning can be performed on scheduled basis to avoid network performance impacts.*
- *NIST-approved tools that are compliant with Security Content Automation Program (SCAP) standards*
- *Identify rogue systems, applications and services*
- *Inventory commercial software to use as evidence to support annual license agreements to avoid overpaying for software licenses*
- *Comprehensive report of all IT assets, by type and associated to FISMA inventory*
- *Use to identify and manage changes, determine system and application dependencies, and support information assurance and compliance efforts.*

Discover Databases and the Sensitive Data they contain through a network discovery of the database environment to create a visual map depicting all interactions among database servers, tables, clients, and applications. Use this information to quickly identify authorized and unauthorized users, applications, and database servers. Using this information, automatically discover and classify sensitive data located inside the databases. Using canned regular expressions, or those devised to the specific needs of your organization, our solution efficiently searches for instances of sensitive data. Once located, they are automatically tagged with meta-data classifications such as “Sensitive but Unclassified”, “PII” or “Controlled Unclassified Information” and added to groups of items with similar properties. The tool can then be used to ensure that appropriate policies are automatically applied to groups of objects with similar properties.



- Deliver a report that identifies the data in use, where it is processed (server and database) and its associated categorizations
- Implement control and auditing of sensitive information
- Using real-time monitoring, understand how data is being accessed from all sources (line-of-business applications, batch processes, ad hoc queries, application developers, and privileged users/administrators)
- Validate system security impact levels (FIPS 199) based on the information found in databases

Implement Solutions for Compliance with OMB Memo 06-16

NIST recently published a [Frequently Asked Questions \(FAQ\) for Sensitive Data Extracts](#)⁷. In this FAQ NIST answers common questions regarding the data which must be audited, the information that needs to be contained in the audit log, and provides approved methods for verifying that extracted data is either still required or has been deleted. Our solution addresses these requirements to enable your organization to rapidly identify the sensitive data, monitor and log the extractions and provide a web-based means to manage continued need or verification of deletion.

Using database access and monitoring tools ensure that appropriate policies are automatically applied to groups of objects with similar properties.

- Using real-time monitoring capture events which trigger auditing for sensitive data extracts based on your data and thresholds
- Produce actionable reports for data owners / custodians which indicate sensitive data extracts along with expiration date. Report on users that have extracted data beyond expiration date
- Provide a web-based interface and work flow to validate and approve continued need and/or certification that data has been deleted.

DB User Name	Source Program	Database Name	Returned Data	Records Affected (Desc)
BENJI	SQLPLUS@OSPREY PII	*****-9012-3450		441
BENJI	SQLPLUS@OSPREY PII	*****-9012-3450		882
BENJI	SQLPLUS@OSPREY PII	*****-9012-3450, *****-9012-3451, *****-9012-3452, *****-9012-3453, *****-9012-3454, *****-9012-3455, *****-9012-3456, *****-9012-3457, *****-9012-3458, *****-9012-3459		882
BENJI	SQLPLUS@OSPREY PII	*****-9012-3451, *****-9012-3451, *****-9012-3451, *****-9012-3451, *****-9012-3451, *****-9012-3451, *****-9012-3451, *****-9012-3451, *****-9012-3451, *****-9012-3451		882

Through these approaches and solutions, organizations can address the following requirements and common security weaknesses:

- ✓ Discover and inventory your network assets and be alerted to changes
- ✓ Inventory and classify your sensitive information and accurately describe your information inventory
- ✓ Identify suspicious activities and incidents and speed analysis and reporting



⁷ csrc.nist.gov/drivers/documents/OMB/OMB-M-07-16-Data-Extract-FAQ.pdf

- ✓ **Create and manage required audit trails and provide efficient means of review**
- ✓ **Implement required security controls for information and databases in accordance with system security impact levels**
- ✓ **Comply with the requirements of OMB Memo 06-16**
- ✓ **Implement controls to support information sharing to permit access to required data and maintain an audit trail**

Implement Enterprise Data Classification and Protection Solutions

Recent attacks have demonstrated that even well managed defenses in depth can be bypassed through introduction of malicious code or user error. These incidents have shown that defining the edge of your network and ensuring adequate protection has become increasingly difficult. CIOs are constantly challenged to deliver data faster to a wider set of devices and business partners while trying to keep pace with new threats that require implementing blocking and other controls at the perimeter. As a result the traditional model becomes more impractical and ineffective.

Organizations must transition to a risk-based mission protection approach where agency missions and business functions drive security requirements and associated safeguards/countermeasures. Following this approach, agencies must architect infrastructures, systems and applications to be highly flexible so they can adapt to future threats and need for information sharing. Mission and business owners can then focus on acknowledgement and acceptance of mission risk.

One way to support this new paradigm is to have security travel with the data, as opposed to relying strictly on hardened network perimeters. There are alternative approaches to implementing this new paradigm that involves the identification, classification and protection of sensitive data. These alternatives must be examined within the context of your agency's operation, infrastructure, and security architecture to determine the combination which provides the best value to your agency.

SECURE|IT offers consulting, design and implementation services for data classification and protection solutions. Provided below is a brief description of the different, and sometimes complementary approaches along with the value of each and some considerations which must be taken into account when deciding on a strategy.

Approach	Value	Considerations
<p>Policy-based approach to discover and categorize data based on metadata and agency-specific rules and policies.</p> <p>Automate encryption of email and documents at the desktop based on data categorization / classification.</p>	<p>Combining these solutions can enable an agency to automate classification and protect it over multiple communication channels.</p>	<p>Discovery of sensitive data can be a difficult task since data can be spread across the infrastructure and applications.</p> <p>Typically focused on unstructured data thereby requiring another solution for databases.</p> <p>Each Agency must define and maintain the keywords, phrases or patterns of its sensitive data for automated tagging.</p>

Approach	Value	Considerations
<p>Centralized management and enforcement of data security also known as digital rights management (DRM)</p>	<p>Federated control and enforcement of classification and data management policies.</p> <p>Encrypt sensitive when at rest or in transit ensuring protection is not removed by end-users</p> <p>Enforce information retention policies by deleting information per records management guidelines.</p>	<p>Users may be required to select or in some manner specify classification of information they produce.</p> <p>Requires all parties to interoperate with central policy/rights server</p> <p>Can introduce impacts to interoperability and information sharing.</p>
<p>Leverage native database security and auditing features. Products such as Microsoft SQL server and Oracle offer features for monitoring user and DBA activity.</p>	<p>Implementing control, auditing and monitoring at the database level enables granularity to low levels offering fined tuned control.</p>	<p>Commercial database management products lack the policy management, reporting, monitoring, and analytics features required without add-on products</p> <p>Cost associated with implementing and operating these features.</p>
<p>Real-time monitoring of databases using policy-based controls and/or anomaly detection to detect and prevent unauthorized access or extraction.</p>	<p>Detect and prevent unauthorized access to databases.</p> <p>Track database extracts</p> <p>Demonstrate due care of data for compliance</p>	<p>Solutions can be limited in the databases and applications supported.</p> <p>Technology varies on its ability to integrate into an open, federated security management infrastructure.</p>
<p>Monitor network perimeter for sensitive data, blocking or encrypting when needed (frequently referred to as data loss prevention (DLP)).</p>	<p>Can be deployed in relatively short period of time.</p> <p>Provides insights into the data that is in use, transmitted and to whom it is shared.</p>	<p>Information can already be leaked to other parts of the infrastructure before detection.</p> <p>Current trend is to integrate this technology with protection at the storage level.</p>
<p>Protect data at rest (DAR) on fixed and mobile media through encryption.</p> <p>Can be deployed in full disk encryption or select file encryption.</p>	<p>FIPS 140-2 validated encryption of data.</p> <p>Ability to destruct data on device based on agency-defined criteria.</p>	<p>Operations must perform centralized policy management, credential issuance and additional password resets.</p> <p>Users can bypass encryption and controls.</p>
<p>Control access from end points so only authorized applications can be accessed and only authorized devices can connect to agency networks and servers</p>	<p>Enforce security policies that prevent known and unknown threats from executing, such as malware, viruses, spyware and zero-day threats.</p> <p>Control and monitor the flow of inbound and outbound data.</p> <p>Provide an audit trail of all data that is copied to and from removable devices.</p>	<p>Can place additional demands on operations to keep pace with changes in applications and devices.</p>

About SecureIT

SecureIT helps private and public sector clients manage technology risks and create value through effective practices in IT security. SecureIT provides services and solutions in the areas of Cybersecurity, Information Assurance, Governance & Compliance, IT Audit, and Security Training. SecureIT designs enterprise security programs, implements best practices and assesses technology implementation for security risk. Professionals with industry knowledge and technical expertise devise strategies and solutions to reduce risk, increase efficiency and overcome the challenges of compliance. Located in Reston, VA, SecureIT serves clients in the Federal government including; DISA, HHS, DOJ, Treasury, Commerce, USAID, Education, DHS, and IMF as well as the private sector with clients such as Freddie Mac, CSC, FINRA, and E*TRADE.

For more information, call 703.464.7010, email info@secureit.com or visit www.secureit.com

Notice

The SECURE|IT logo, and all page headers, footers and icons are trademarks or registered trademarks of SecureIT Consulting Group. Other company names or products mentioned are or may be trademarks of their respective owners. Information in this document is subject to change without notice.