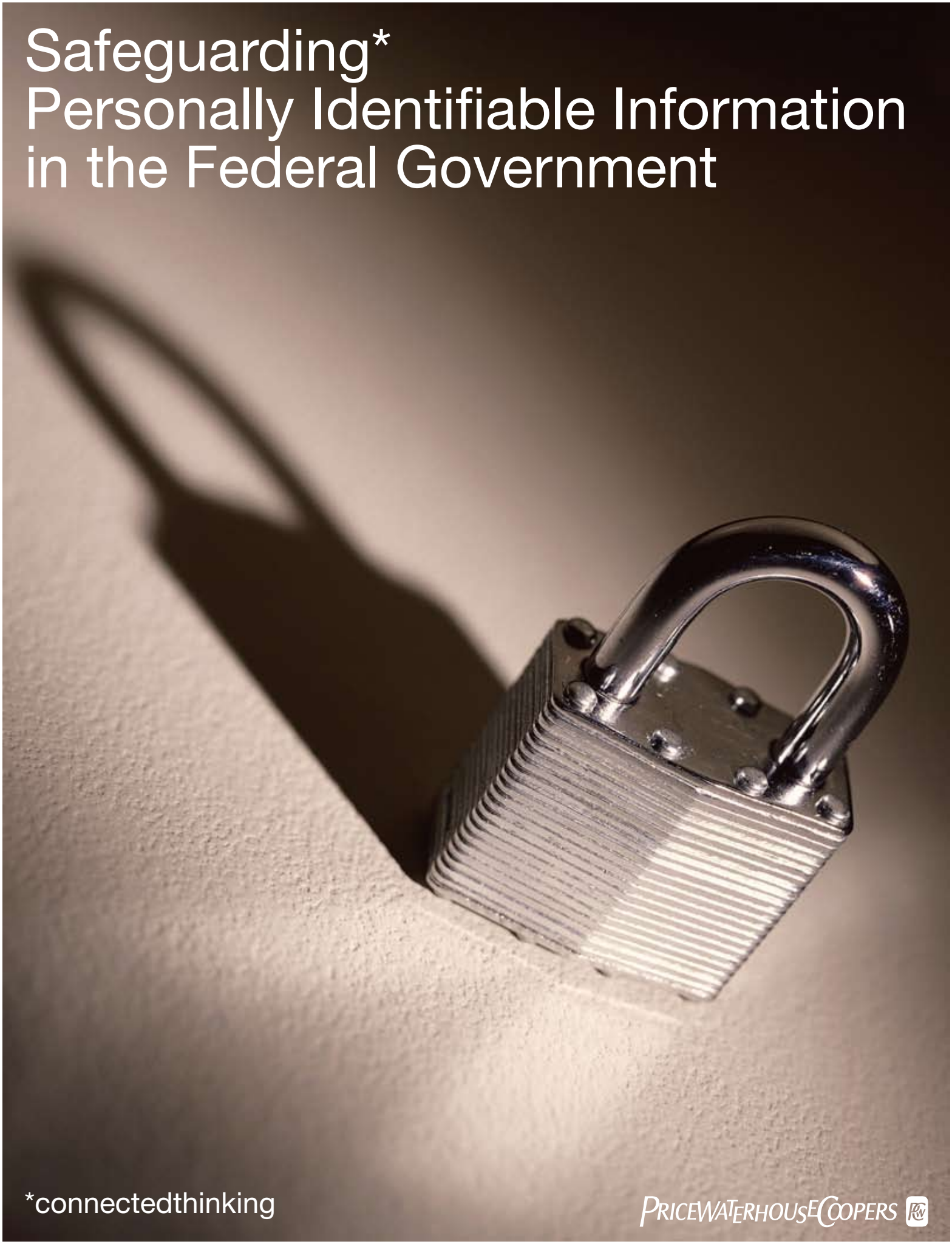
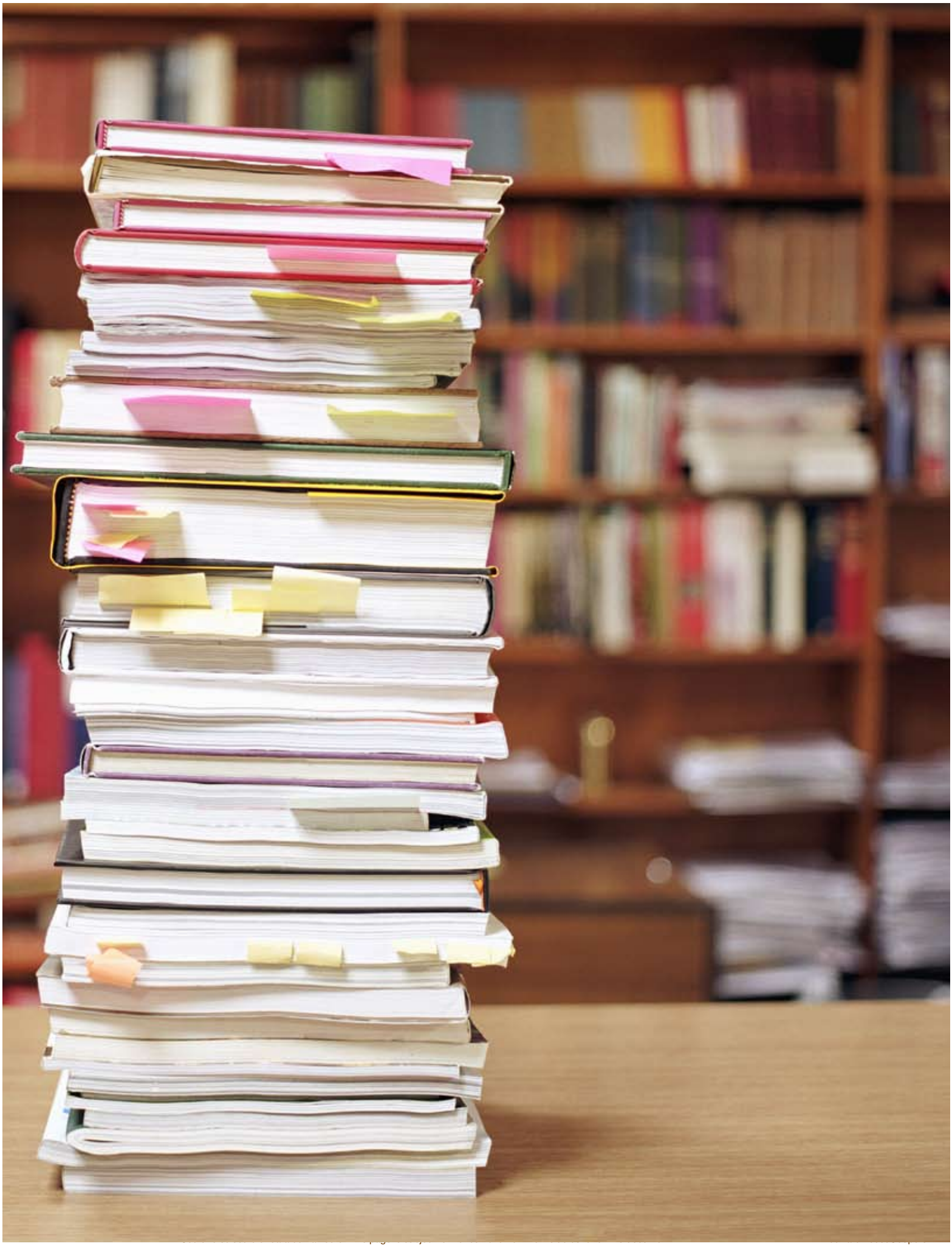
Safeguarding* Personally Identifiable Information in the Federal Government



*connectedthinking

PricewaterhouseCoopers

Table of Contents



Introduction

Recent well publicized actual and potential disclosures of U.S. citizens' personally identifiable information (PII) by the Federal Government and its employees have resulted in heightened scrutiny of agency information security and privacy programs. The Administration, Congress, Office of Management and Budget (OMB), Government Accountability Office (GAO), Offices of Inspector Generals (OIGs), the press and the U.S. public are all paying increasing attention to the Federal Government's collection and use of PII. Safeguarding PII is a major undertaking that requires measures beyond basic compliance with applicable laws and regulations. Protecting PII calls for wide-spread collaboration across agencies and a consistent approach. It also requires stewards of PII to understand and fulfill their responsibilities to protect such information. The Federal Government collects information and maintains records on virtually everyone to better serve and protect the citizens and non-citizens (e.g. legal permanent residents and visitors) of the U.S.[1] This information is associated with every point at which the Federal Government touches the life of any citizen and non-citizen, and generally PII. Due to the volume, nature and sensitivity of PII, the Federal Government must exercise great vigilance to adequately safeguard this information.

What is Safeguarding?

Within the context of the Federal Government and PII, safeguarding refers to protecting PII from loss, theft or misuse while simultaneously supporting the agency mission. Safeguarding PII encompasses a variety of ever-changing and interrelated activities from policy development, implementation, and review; to incident prevention, monitoring, and management; to stakeholder collaboration, and education and awareness. Furthermore, effective safeguarding employs a robust, strategic framework that matches an agency's privacy protection efforts to the nature of its daily operations. Safeguarding PII requires great diligence and proactiveness, and significantly enhances the overall privacy posture throughout the Federal Government.

Safeguarding in Review

One of the greatest risks to collecting PII is losing control of the information, whether by inadvertently sending the information to the wrong party, loss or theft of media containing the information (e.g. a printed report or electronic media), or a network infiltration, all of which may result in a privacy breach. Such a breach could also place citizens and non-citizens at risk of identity theft, thus increasing the need for the Federal Government to not only effectively safeguard PII, but to be in the position to respond quickly when a breach does occur. Additionally, when an incident occur, it's not only a political and reputation problem for an agency but also a significant financial one. For example, in May 2006 when the Veteran's Administration (VA) lost a laptop containing PII on 26.5 Million veterans and their families it was estimated to cost the VA $160 Million for free credit monitoring and $25 Million to set up a call center and notify veterans[2]. Resultant to the privacy breaches within the past several years, additional complex and stringent regulations regarding the protection of PII have been issued.

[1] Source: "Guarding Privacy in the Federal Government: A Holistic Approach" February 2007, (http://www.pwc.com/extweb/pwcpublications.nsf/docid/351D8C55FDB3D7E28525728E006416EB)

[2]Christopher Lee and Zachary Goldfarb, "Stolen VA Laptop and Hard Drive Recovered," The Washington Post, June 30, 2006.

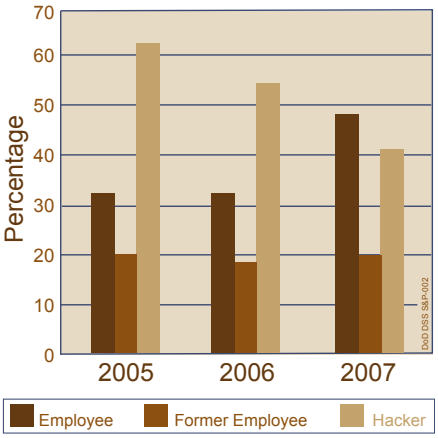


Figure 1: Increasing Percentage of Employee Incidents

Although making strides to protect against privacy breaches, Federal Information Security Management Act (FISMA) reports indicate the prevalence of privacy breaches throughout the Federal Government. According to the Fiscal Year (FY) 2007 FISMA Report to Congress[3], twice as many incidents, 12,986, were reported to the Department of Homeland Security (DHS) than in FY 2006. Of these reported incidents, approximately 29% may have involved PII wherein 2,321 were due to unauthorized access and 3,305 to improper usage, of which one-third can be attributed to inadvertent PII disclosures. In 2007, the Global State of Information Security Survey 2007[4], a worldwide study by PricewaterhouseCoopers, CIO magazine, and CSO magazine, also reported that 48% of respondents attributed breaches to employee compromises and possible inadvertent disclosures; up from 33% in 2005 (see Figure 1). These statistics suggest continuing issues in privacy compliance, as well as possible inconsistencies in implementation of protection methods throughout multiple industries. According of the GAO, the Federal Government is one of the industries struggling with these types of issues. Of the breaches noted in Appendix II of the GAO's January 2008 report, titled "Information Security: Protecting Personally Identifiable Information," almost 25% involved missteps or malicious actions by employees[5].

The potential adverse impacts of a privacy breach are a key driver in motivating the Federal Government to enhance efforts to comply with privacy regulations and protect the privacy of both citizens and non-citizens. Consequences and repercussions include, but are not limited to the following:

- Criminal penalties (e.g. fines and/or imprisonment);
- Reduced funding and budget;
- Termination of government programs;
- Significant remediation costs and extended recovery times
- Loss of public trust; and
- Tarnished reputation detracting from the ability to attract and retain quality personnel.

Generally, privacy issues occur in multiples, which can compound the impact. Therefore, Government agencies must continually extend their privacy efforts to promote collaboration and awareness as well as implement policies and procedures comparable to the context within which they collect and utilize PII.

[3]See OMB "Fiscal Year 2007 Report to Congress on Implementation of the Federal Information Management Security Act of 2002" (http://www.whitehouse.gov/omb/inforeg/reports/2007_fisma_report.pdf).

[4]Source: "Global State of Information Security Survey 2007," a worldwide study by PricewaterhouseCoopers, CIO magazine and CSO magazine.

[5]See GAO " GAO-08-343 Information Security: Protecting Personally Identifiable Information" (http://www.gao.gov/new.items/d08343.pdf).

Privacy and Security Compliance

Listed below are examples of recent OMB Memoranda focused on safeguarding PII:

- M 06-15, "Safeguarding Personally Identifiable Information"
- M 06-16, "Protection of Sensitive Agency Information"
- M 07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information"
- M 07-19, "FY 2007 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management"
- M 08-09, "New FISMA Privacy Reporting Requirements for FY 2008"

These OMB mandates aim to further enhance the safeguarding practices across the Federal Government in coordination with guidance issued by the National Institute of Standards and Technology (NIST) (e.g. Special Publications 800-37, 800-53a revision 2, and Federal Information Processing Standards 140-2, 199 and 200).

Addressing Safeguarding Requirements

Federal privacy requirements, and specifically, requirements for safeguarding PII, are spread across multiple laws, such as the Privacy Act of 1974, E-Government Act of 2002 (Section 208), and Title III, FISMA. OMB also continues to issue mandates focusing on safeguarding PII, requiring agencies to develop and implement specific safeguarding policies and procedures, track data flows of PII, develop and administer training to promote education and awareness, and appropriately report incidents involving PII (see sidebar: Privacy and Security Compliance). In our experience, we find that the most successful strategies for safeguarding PII include incorporating agency-wide collaboration with stakeholders, proactively identifying and addressing existing and emerging challenges, promoting privacy policies through on-going education and awareness, continually reviewing and updating privacy policies, and taking into consideration the dynamic nature of agency operations. This extends beyond basic compliance and takes into consideration the ethical obligations of the Federal Government to protect the privacy of citizens and non-citizens. Per the requirements defined in the various laws and mandates, we believe the key activities discussed in the following section are essential to safeguarding PII and implementing privacy protections.

Elements of Safeguarding

There are a number of detailed requirements across multiple areas the Federal Government must address to properly safeguard PII, and there are often interdependencies between requirements. We believe Federal agencies can significantly enhance their PII safeguarding strategies by incorporating adequate privacy protections in the following areas:

- Organization
- Policies, Procedures, and Controls
- Education and Awareness
- Collection
- Data Management
- Monitoring and Reporting
- Managing Incidents and Breaches

Several of the major requirements, as well as additional success factors, are described for each element and any subcomponents listed in the following sections. Although it is a critical element of privacy and safeguarding, information security is not addressed in this publication.

Organization

Many Federal employees and contractors work with PII everyday and are a critical component to safeguarding PII. OMB requires agencies to develop privacy rules of behavior, communicate these behaviors effectively throughout the agency, and provide adequate training to all agency personnel, both employees and contractors. The intent is to develop behaviors that all personnel acknowledge and are responsible for adhering to in their every day activities, similar to a code of conduct. These rules of behavior should promote all personnel's understanding of the importance of safeguarding PII, their roles and responsibilities in protecting such information, and the consequences for failed compliance. In addition to a broad set of rules for all agency personnel, agencies should consider more specific responsibilities for various staff levels (e.g. supervisory and non-supervisory) and job functions (see sidebar: Examples of Employee Privacy Rules of Behavior, Responsibilities and Consequences).

Privacy rules of behavior must explicitly detail roles and responsibilities (specific to the agency's operations). Clearly defined roles provide direct accountability to agency personnel for adequately safeguarding PII and properly handling incidents or breaches. In order to be effective, these policies must be communicated to and understood by all personnel performing duties on behalf of the agency.

Policies, Procedures, and Controls

One of the major challenges to privacy policy is addressing the disparate privacy requirements spread across various laws, regulations, and guidance. In addition to the specific privacy requirements, there is a web of requirements that directly and indirectly support privacy efforts and may already be in place (e.g. FISMA, Paperwork Reduction Act, OMB Exhibit 300s, and OMB A-11). Effectively managing this complex requirements landscape is necessary to create a solid framework for safeguarding PII and handling privacy breaches (*see sidebar next page: Breach Notification Policy*). One approach we found successful is to conduct a gap analysis of existing policies and procedures against privacy requirements. Through this process, agencies map policies to privacy compliance policies already in place. In addition to providing agencies a way to demonstrate compliance, this approach helps agencies identify additional measures needed to satisfy those requirements and take a focused approach to policy development. Additionally, each policy should have an accompanying implementation plan noting timelines and milestones both for deployment and agency compliance (e.g. education and awareness efforts and annual training).

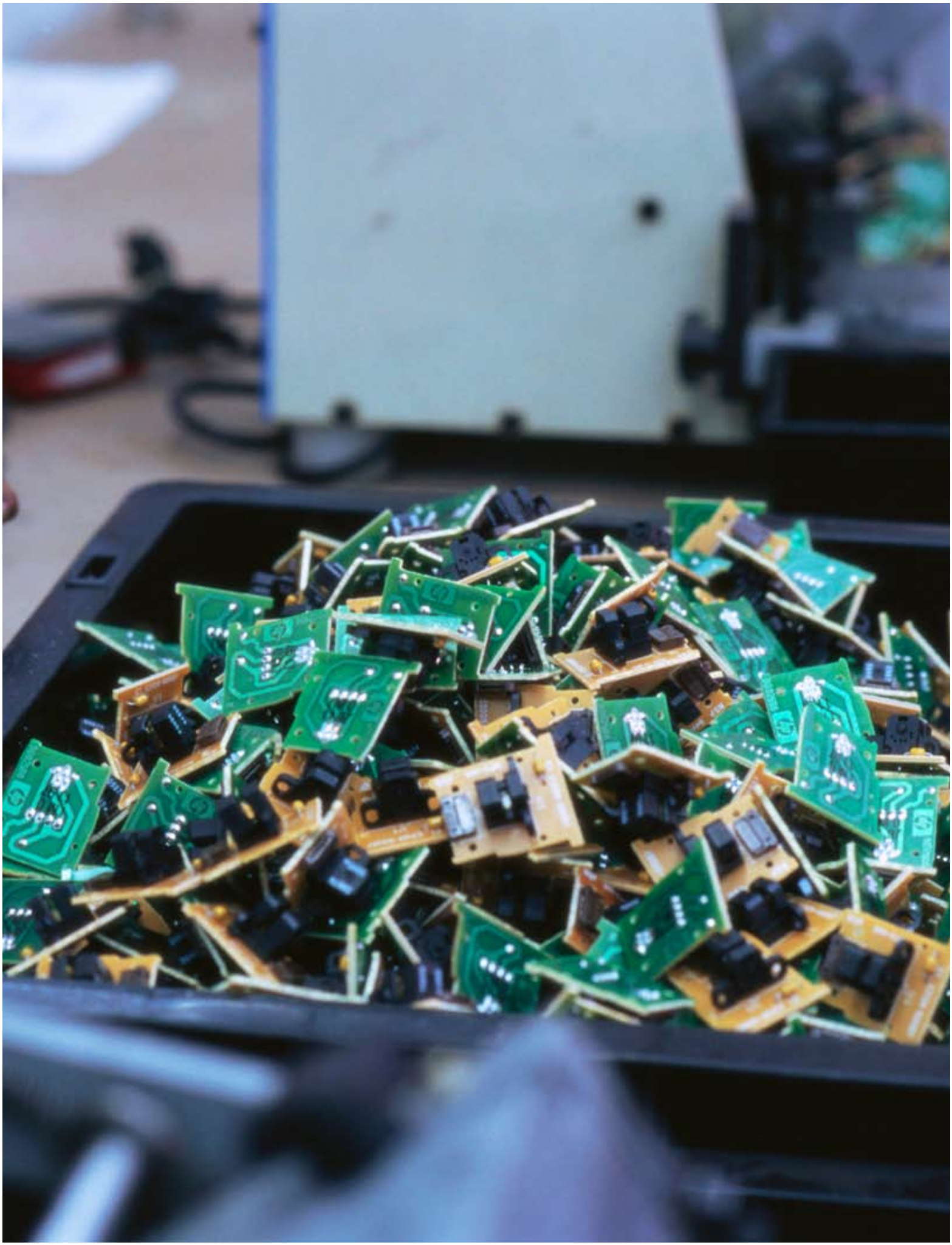
Examples of Employee Privacy Rules of Behavior, Responsibilities and Consequences

All Personnel	Supervisory Personnel
• Adherence to access control requirements (e.g. "Need to Know" and remaining within the purview of your assigned duties) • Limit personal use of government-issued equipment • Keep a clean working environment (e.g. lock files in a cabinet when leaving your desk) • Report suspicious computer activity or incidents (e.g. files disappearing, LED lights functioning improperly, lost thumb drive)	• Lead by example to foster an environment of privacy protection • Determine access necessary for supporting personnel • Promote training opportunities to supporting personnel • Conduct random clean desk checks

Agency Consequences and Corrective Actions for Failed Compliance

- Temporary loss of access for personnel to agency information systems (e.g. for a period of time or until the employee successfully completes additional training)
- Fines, probation, or other adverse administrative actions

[6]See OMB M 07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable



Breach Notification Policy

Per OMB M 07-16, agencies were required to implement an external breach notification policy by September 2007 to address the following issues:

- Identification of covered individuals
- Harm to individuals produced by the breach
- Criteria for determining the impact of the breach and whether the breach warrants external notification, taking into account the sensitivity of the agency's operations
- Procedures for providing notification
- Timeliness, source, and contents of the notification
- Method of notification delivery

Upon reviewing efforts to comply with this requirement, OMB recommended in the 2007 annual FISMA report that agencies with policies in place also develop notification templates, prepare news releases, and increase compliance with Section 508 of the Rehabilitation Act to accommodate individuals who are hearing or visually impaired. The ultimate goal is for agencies to develop and implement standard operating procedures that position them to mobilize more efficiently when responding to a breach.

Education and Awareness

All agency personnel must be knowledgeable of privacy policies, and more importantly, they must be aware of their responsibilities and held accountable. When implementing privacy protections, PwC has seen that robust education and awareness "campaigns" centered around on-going communication prove more successful than periodic training alone. An education and awareness program is essential when implementing measures and practices to safeguard PII. In addition to periodic training, it is important that safeguarding messages are communicated regularly to agency personnel. Examples education and awareness program elements include developing interactive and dynamic training, hosting information sessions, attending and participating in speaking engagements, distributing news releases relevant to safeguarding issues, sending agency-wide email notifications, and posting information materials throughout agency offices. These efforts reinforce individual participation, responsibility and accountability at all levels of the agency.

Collection

Simply stated, the more data an agency collects, the more it must protect. Designated privacy personnel should collaborate with other agency PII stakeholders, such as the Chief Information Officer and Chief Information Security Officer, to review and streamline collection practices and routine uses to meet agency operation requirements and enhance the overall privacy posture of the agency.

Over time, agency operations change and new processes develop, which may result in duplicative volumes and unnecessary uses of PII. Information may also become outdated or obsolete. These extraneous PII holdings make Federal agencies more susceptible to the risk of a breadth. To mitigate these risks and vulnerabilities, OMB requires agencies to develop a plan to examine, periodically review, and reduce PII holdings[6]. The intent is to limit the collection and use of PII necessary to accomplish the agency's mission. Similarly, OMB privacy requirements mandate that agencies must develop plans to eliminate the unnecessary use of social security numbers (SSNs). In both cases, agencies should first inventory PII holdings and document PII data flows to aid in identifying and eliminating duplicative and unnecessary holdings. One of the most challenging and over-looked steps in conducting a PII inventory is taking into account data extractions from various systems.

Data Management

Subsequent to collecting PII, it is important that agencies ensure the information is used appropriately and only for the purposes for which it was originally collected. Acceptable uses of PII should be clearly defined in the routine uses in System of Records Notices (SORNs) and be commensurate with the potential impact to the individual and agency if compromised. Federal agencies should also make certain that any personnel, to include contractors, with access to PII have a clearly defined "need to know." In other words, personnel should only be granted access to PII to perform official duties as assigned, and once no longer needed, access

[6]See OMB M 07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information" (http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf).

should be terminated. For systems that do not provide means of granularly restricting access, additional policy and educational measures must be implemented to further stress the importance of personnel only accessing information specific to their tasks.

To effectively protect PII, it is important to know what information is collected and retained, the impact designation of the information, and information system interconnectivity. PII inventories and data flows help agencies monitor and protect against unauthorized access, misuse, loss or theft as well as maintain the confidentiality, integrity, and availability of PII.

Safeguarding practices become significantly more complex when agencies share PII externally. The increased susceptibility of a privacy breach is a risk accepted by all parties involved, but above all, the agency originally responsible for collecting the information should be held accountable. The additional risks and complexities obligate Federal agencies to exercise even greater vigilance to safeguard PII. Federal agencies should make certain that sharing PII with an external agency or third party falls within the purview of the defined routine uses and that appropriate controls are established to adequately safeguard the information. Examples of such controls include, but are not limited to, memoranda of understanding (MOUs) or contracts that require the external entity to safeguard the PII by incorporating specific privacy protections (e.g. encryption, personnel training, and retention clauses) and establishing a chain of command or notification. Not only should the safeguarding requirements be mutually agreed upon, but the collecting agency should periodically audit the external agency to increase accountability and the likelihood of compliance with the terms of safeguarding agreements.

Monitoring and Reporting

Robust and comprehensive safeguarding strategies require processes to continuously monitor, assess and improve safeguarding practices. Periodic reviews and assessments are important, not only in evaluating the success of existing efforts to safeguard PII, but also in identifying and mitigating new risks and vulnerabilities.

In addition to the reporting requirements defined by FISMA and the OMB (e.g. incidents, Privacy Act and redress requests), agencies should develop metrics to gauge the success of all their safeguarding practices and identify points for improvement. Upon identifying any areas needing improvement, agencies should implement remediation and benchmarking processes that support continuous improvement.

Managing Incidents and Breaches

Despite great diligence to implement adequate safeguarding measures, privacy breaches can still occur. In light of this reality, agencies should develop effective strategies and procedures for managing incidents and breaches whether suspected or real. To aid in safeguarding PII, OMB required Federal agencies to develop incident handling policies and procedures (see OMB M 07-16)[7], NIST developed guidance for developing incident response plans[8], and DHS established the United States Computer Emergency Response Team (US-CERT) to help agencies manage, report and respond to incidents and breaches. Specific to safeguarding PII, agencies should use the aforementioned resources to:

- Clearly define and categorize a privacy breach;
- Provide training to all personnel (including contractors) about identifying and reporting a privacy breach;
- Establish standard operating procedures for handling a privacy breach;
- Identify key personnel responsible for responding to a privacy breach; and
- Convene a “lessons learned” to identify the cause of the breach and develop an effective mitigation strategy to prevent future breaches.

Agencies must also develop an effective strategy to notify impacted individuals in the event of a privacy breach. Agencies must work through various scenarios based on the types of information maintained and risks of loss to develop a notification strategy. Factors agencies must consider regarding the timing of notification include national security concerns, adverse impact to the investigation of the breach, and enabling individuals to take their own protection measures. Premature privacy breach notification could adversely impact the investigation of the breach, lessons learned, and the development of effective mitigation strategies to prevent future breaches. These are determinations that should be consistent with the mission and operations of the agency, as well as clearly defined and justified in the agency’s breach notification policy.

[7]See OMB M 07-16 “ Safeguarding Against and Responding to the Breach of Personally Identifiable Information” (http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf)

[8]See NIST SP 800-61 rev 1, “Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology.” (http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf)

Additional Tools for Success

In addition to well implemented privacy protections, agencies can enhance their safeguarding practices with various technologies. One type of technology PwC sees as a valuable data protection tool that aids our clients in safeguarding PII is data loss prevention (DLP) or content monitoring tools. The monitoring controls currently called for under guidance such as NIST 800-37 and NIST 800-53, focus on areas such as system configuration, impact of system changes, access control, tracking system vulnerabilities identified during the C&A process, and auditing. The guidance provided in these documents does not yet address the features available in newer technologies. DLP tools extend monitoring capabilities beyond those typically used for monitoring security controls, and when properly configured, provided capabilities to proactively identify privacy breaches in real-time and even prevent breaches before they occur.

Effective deployment of DLP tools requires a supporting safeguarding framework of policies and procedures. Appropriate rule sets must be developed and implemented, business processes put into place and the systems need to be tuned. However, when used as a component in a comprehensive content monitoring program these tools have proven to be very effective. In addition to serving as policy enforcement tools, they also provide capabilities for re-enforcing awareness and education messages. The techniques DLP tool employ vary, but they generally provide various, customizable, functional capabilities, such as:

- Identifying PII across an agency's network by matching data based on SSNs or other identification number, key words, or specific combinations of data (as defined by the user)
- Tracking data extracts, including those on mobile devices and portable media
- Providing a centralized reporting console with role-based access control
- Providing flexible policy-based deployment enterprise-wide
- Customizing incident response workflows to route and manage incidents based on severity and status
- Incident correlation based on details such as email subject line, file name, and policy
- Collecting files matching policy criteria for use in incident investigations
- Automating enforcement of policies
- Notifying appropriate personnel of policy violations

Content monitoring is the proactive and ongoing examination of data, its use, transmission and storage relative to a defined set of rules. A content monitoring program takes the approach of using people, processes, and technology to establish and impose rules for handling defined types or sets of data. It provides for the ongoing monitoring of compliance with the defined rule set, such as safeguarding requirements, identification and notification of violations of the rules, and a response to violations that mitigates the associated risks.

For example, an agency may require all files containing SSNs to be stored in an encrypted folder and may only allow emailing SSNs to .gov email addresses. If employing a content monitoring tool, rules would be configured to support these requirements. The monitoring tool would then look for files containing SSNs on unencrypted drives and in email traffic. In the event either of these rules is broken, the monitoring tool would execute the defined response. For example, a typical response may include automatically moving a file containing the SSNs and leaving a placeholder to notify the user regarding the new file location and a link to the corresponding policy broken. In the instance of a user attempting to send an email to a hotmail.com address, the content monitoring tool may quarantine the email and send a note to both the user and their manager informing them of the policy violation. Responses may also be configured to contact designated parties, such as the Information Technology department, to investigate further and take any additional measures that may be necessary. Response workflows can be tailored within these tools to meet agency requirements.

Data monitoring programs offer several benefits, such as:

- Building a PII inventory;
- Improving compliance through automated monitoring and response;
- Reducing risk by limiting exposure of PII or other confidential material;
- Determining whether or not an incident actually occurred; and
- Minimizing response time and expense through automated notification and logging of incidents.

In our experience, the time and effort to deploy DLP tools provide a number of benefits to organizations in their safeguarding practices. They are a key component to the future of safeguarding.

The effective deployment of DLP tools support real-time detection and prevention of privacy breaches which can greatly help the Federal Government reduce the risks associated with privacy breaches. Additionally, the reports gathered from DLP tools can be used to identify new risks to the agency as well as promote education and awareness efforts. Used appropriately, such monitoring tools can help fortify an agency's strategy for safeguarding PII.

Conclusion

Successful implementation of safeguarding practices hinges upon several factors, including, but not limited to, support from senior leadership, employment of adequate internal controls and review processes, and effective communication through continued education and awareness efforts. Furthermore, safeguarding PII entails more than meeting the minimum FISMA and OMB reporting requirements; it requires exercising precaution when handling and protecting PII. Failure to do so could constitute an abuse of authority and trust bestowed upon the Federal Government by those individuals whose information they have collected and are maintaining. Non-compliance could also result in stolen identities, major remediation costs, reduced funding, criminal penalties, and embarrassment for the Federal Government. Beyond minimum compliance requirements, the Federal Government is obligated to safeguard PII on behalf of the citizens and non-citizens. As such, agencies must incorporate appropriate, comprehensive privacy protections into their practices, and continually review and prepare for new, emerging challenges.

About PricewaterhouseCoopers

PricewaterhouseCoopers (PwC) has over 2000 professionals based in the Washington Metro Corridor. Our mission is to become the U.S. Federal Government's preferred provider of advisory and assurance services. We help government agencies solve complex business issues, manage risk and add value to performance through our comprehensive service offerings in financial management, program management, operations improvement, and security and data management, all of which are delivered seamlessly throughout the world.

We build relationships with our government clients by providing outstanding services based on quality and integrity. Our networks, experience, industry knowledge and business understanding distinguish the way we work. Within our own teams and with our clients, we are collaborative, open and direct. We are not content with standard solutions. We push ourselves and our clients to think harder, to understand all of the consequences, and to consider new perspectives.

ACKNOWLEDGMENTS:

PwC prides itself on the concept of Connect Thinking. For this paper, we drew support and expertise from PwC staff with varied experience and knowledge from around our firm. A core group of PwC staff worked diligently to help produce this publication. These team members include:

Privacy subject champions:

Scott McIntyre
PwC Managing Partner
703.918.1352

Jack Johnson, Jr.
PwC Principal
703.918.1303

Julie Nethery, CIPP/G
PwC Federal Privacy Lead
703.918.3186

Privacy project team:

James Golihar
PricewaterhouseCoopers

Jonathan Moore, J.D., MSEC
PricewaterhouseCoopers

Matthew Liberty
PricewaterhouseCoopers

Eliza Nagle
PricewaterhouseCoopers

pwc.com/usgov/privacy