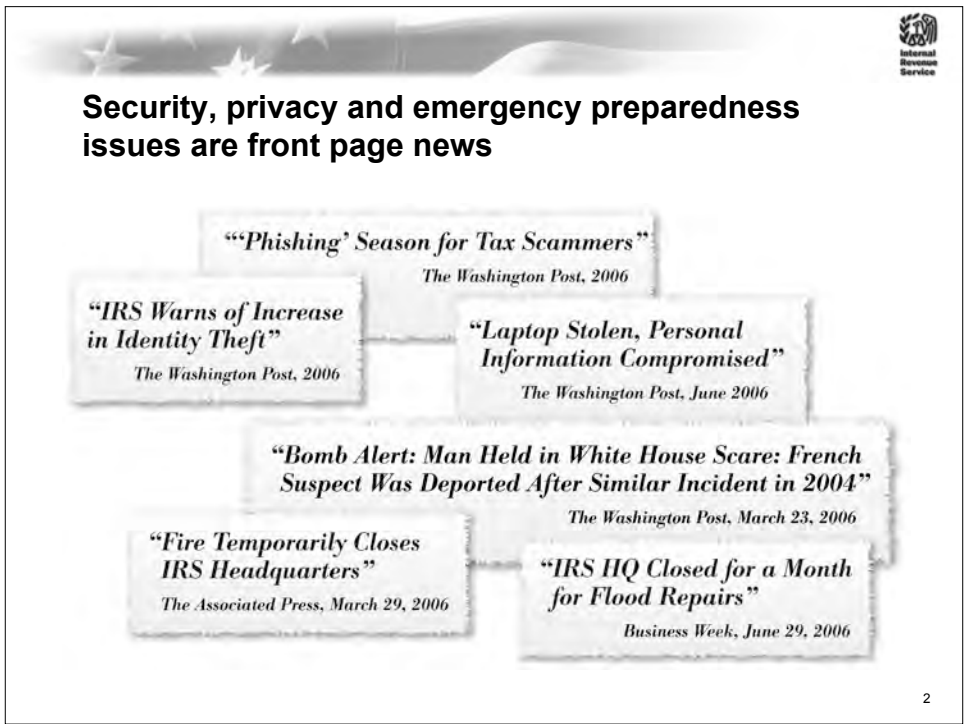



Internal Revenue Service

Mission Assurance and Security Services

Dan Galik, Chief

*Federation of Tax Administrators
Computer Security Officer Conference
March 2007*

Security, privacy and emergency preparedness issues are front page news

*“Phishing’ Season for Tax Scammers”
The Washington Post, 2006*

*“IRS Warns of Increase in Identity Theft”
The Washington Post, 2006*

*“Laptop Stolen, Personal Information Compromised”
The Washington Post, June 2006*

*“Bomb Alert: Man Held in White House Scare: French Suspect Was Deported After Similar Incident in 2004”
The Washington Post, March 23, 2006*

*“Fire Temporarily Closes IRS Headquarters”
The Associated Press, March 29, 2006*

*“IRS HQ Closed for a Month for Flood Repairs”
Business Week, June 29, 2006*

2

Computer systems and data are critical assets for IRS to achieve its mission

"Infamous computer hacker pleads guilty in deal with government"

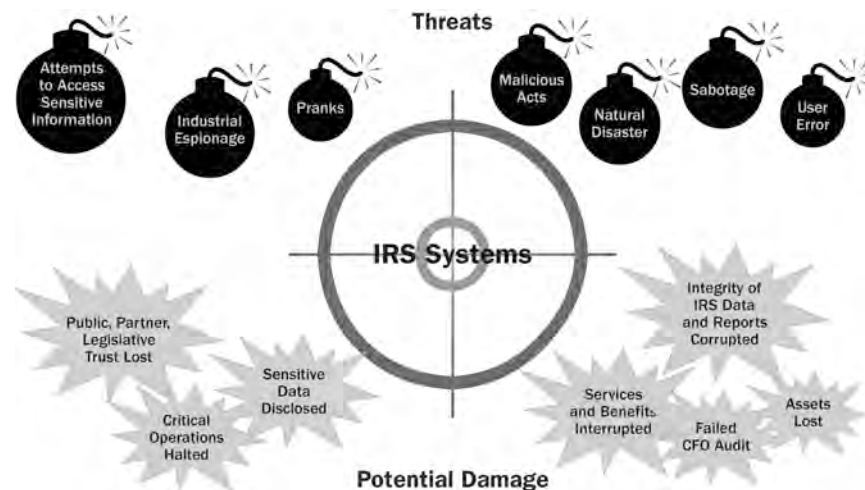
"GAO Warns of Social Security Number Theft"

"9.9 million Americans victims of Identity theft last year"



- ▶ Requirement for a high degree of public confidence that IRS systems and data are secure
- ▶ E-Government and electronic tax administration are major thrusts
- ▶ Threats are more sophisticated, complex and expand exponentially
- ▶ Boundaries more vague – significant interaction with partners
 - Tax preparation and submission
- ▶ Increasing scrutiny and regulation
- ▶ Increased amount of sensitive information handled by IRS systems

Security Threats Require a "Total Protection" Approach to Security





Security “Convergence”

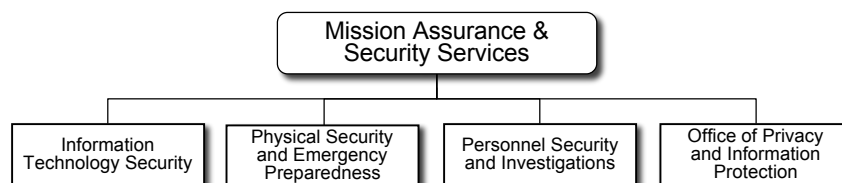
- ▶ A comprehensive and integrated security strategy where all security disciplines (computer security, physical security, personnel security, etc...) contribute to reducing risks
- ▶ Today’s threats to our mission, functions, and operations come from more than just the electronic world
- ▶ Security convergence approach promotes information sharing and collaboration among disparate security functions
- ▶ Security technology is converging, as proprietary systems are being replaced with a centralized, IP-based security management system. Closed-circuit TV, door alarm controls, access card control systems, sensors, alarm monitoring, and even building control systems such as HVAC and lighting, are all moving onto the network.

5

Organization Charts



Mission Assurance and Security Services: *Security, privacy and emergency preparedness are all under one organizational umbrella*



6



In support of the IRS mission to provide American taxpayers with top quality service, the IRS developed a security and privacy strategy comprised of the following key elements:

- ▶ Identify critical (essential) business processes that support the core missions and functions of the service
- ▶ Identify assets (people, buildings, facilities, data, IT systems) that support critical, essential functions
- ▶ Apply appropriate cost effective security protections based on risk
- ▶ Monitor operational effectiveness of security protections
- ▶ Test plans and capabilities for the recovery/resumption of critical operations
- ▶ Enhance security and privacy education, training, and awareness

7



The Federal Information Security Management Act (FISMA)

All Federal Departments and Agencies Shall:

Be responsible for ensuring that senior agency officials provide information security for the information and information systems that support the operations and assets under their control

Each Agency Shall:

Develop and implement an agency wide information security program (approved by OMB)

8

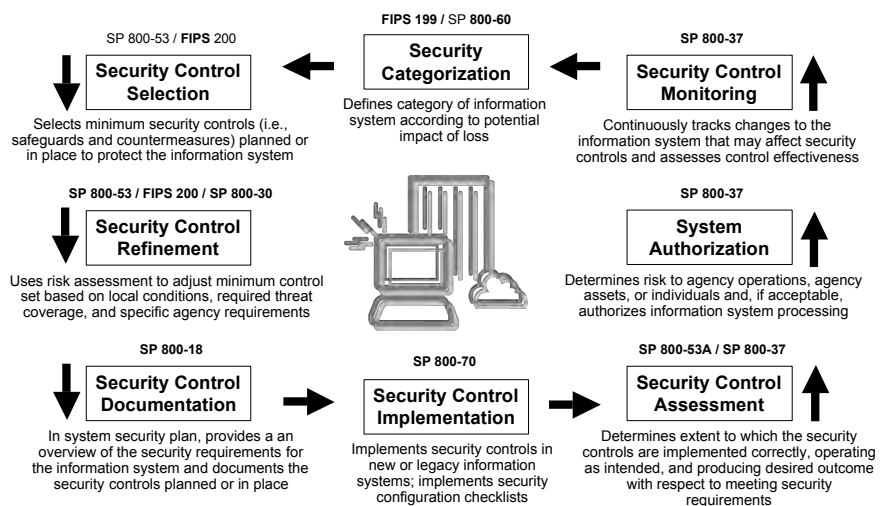
OMB's FISMA guidance dictates that Agencies must:

- ▶ Incorporate security into their business systems
- ▶ Prioritize key systems that are critical to agency operations
- ▶ Make security costs explicit in all IT investments and capital programming
- ▶ Implement a cost effective risk management approach to security
- ▶ Develop a security plan for each system
- ▶ Assign responsibility for the security of each system
- ▶ Annually review and test security controls, including associated contingency plans for business continuity and disaster recovery
- ▶ Formally authorize processing for each information system



9

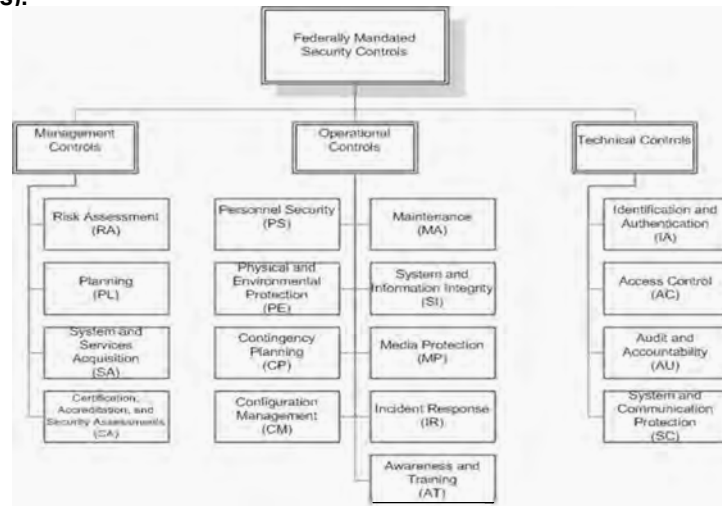
The NIST Framework Provides the Foundation For the IRS IT Security Program.



10



NIST SP 800-53 (and FIPS 200) Identify the Mandatory Security Controls Required for all Federal Information Systems. (Foundation for Pub 1075 Updates).



IRS has implemented a broad-based, enterprise-wide Information Technology (IT) Security Program

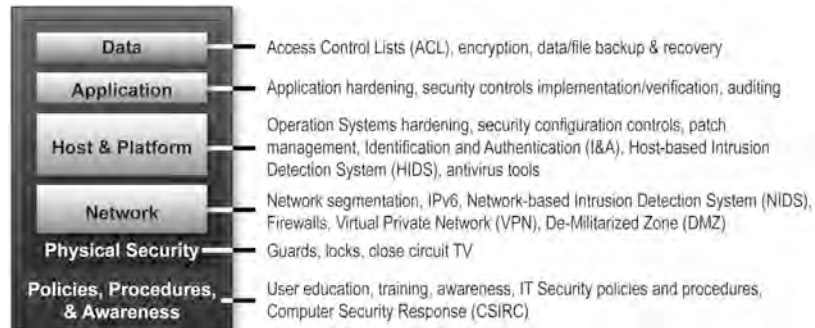


Links in the Chain: Management, Operational, and Technical Security Controls

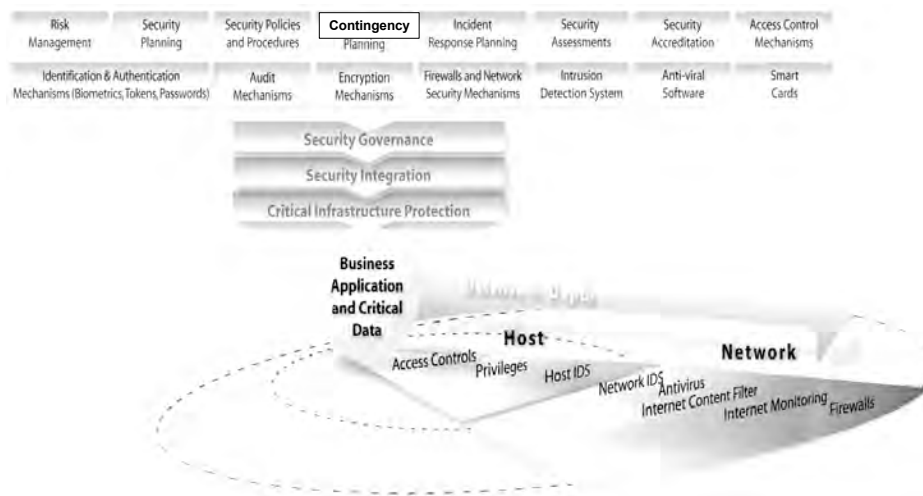
- ▶ Risk management
- ▶ Security planning
- ▶ Security policies and procedures
- ▶ Contingency planning
- ▶ Incident response planning
- ▶ Security Assessments
- ▶ Security Accreditation
- ▶ Access control mechanisms
- ▶ Awareness and Training
- ▶ Identification and authentication mechanisms (biometrics, tokens, passwords)
- ▶ Audit mechanisms
- ▶ Encryption mechanisms (including PKI)
- ▶ Firewalls and network security mechanisms
- ▶ Intrusion detection systems
- ▶ Anti-viral software
- ▶ Smart cards

IRS implements a layered, defense-in-depth approach to IT Security

- ▶ Using a layered approach:
 - Increases an attacker's risk of detection
 - Reduces an attacker's chance of success



The IT Security and Privacy Technical Strategy





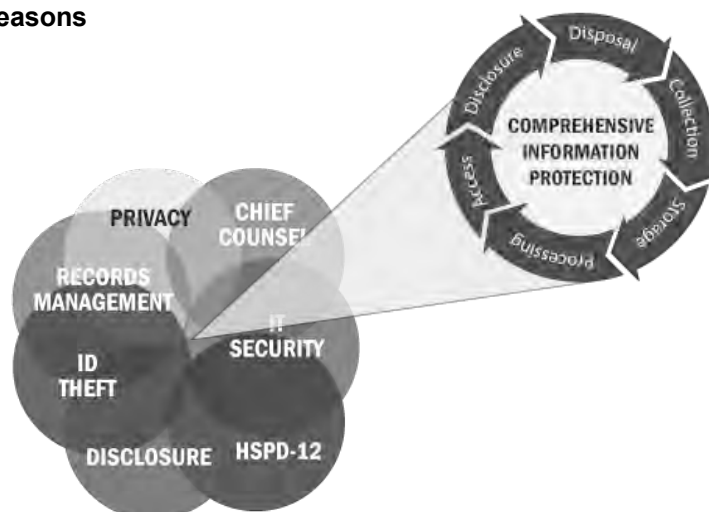
FY2007 Top IT Security and Privacy Priorities for IRS

- ▶ Encryption of Data
 - Includes stored data and data traded with external stakeholders
- ▶ Secure and Control IT Assets
 - Accurate inventory; security configuration control;
- ▶ Integration of Security and Privacy Practices into Enterprise Lifecycle (ELC) Systems Development and Governance Processes
 - Build all new IT applications systems to meet FISMA/NIST security and privacy standards
- ▶ Focus on Material Weaknesses
 - Enhance systems security auditing; disaster recovery capabilities
- ▶ Enable Operations to Efficiently Ensure Security Across the Enterprise
 - Enhance the suite of automated security tools to support network operations, (security patch management; network security monitoring; vulnerability assessment/remediation, etc..)

15

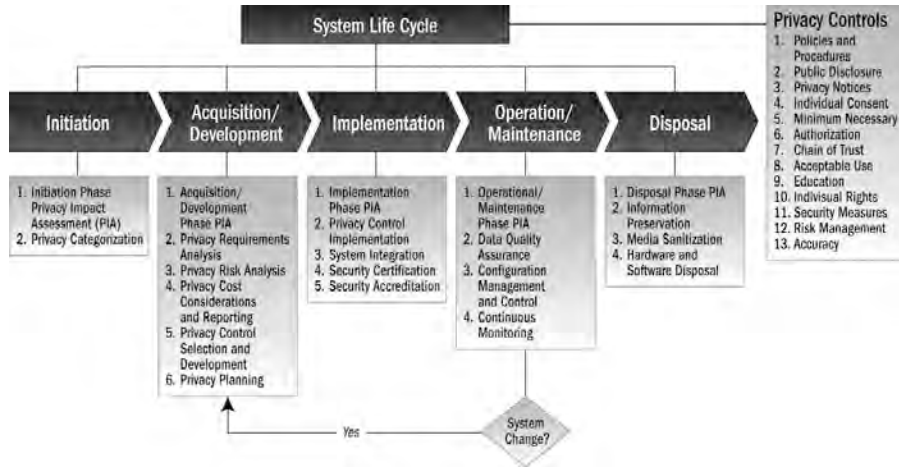


At the IRS, Privacy and Identity Protection is more than just securing data. It is about enabling taxpayer and employee confidence by ensuring the right people see the right data in the right places for the right reasons

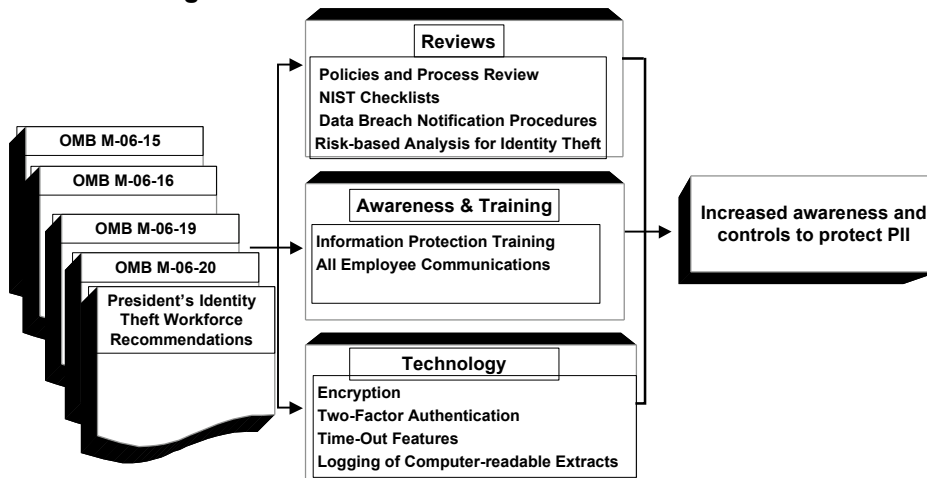


16

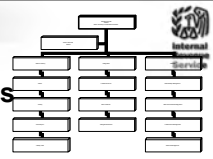
Just like security, embedding privacy throughout the System Life Cycle enables a cost-effective, comprehensive approach to risk management



Several Recent Federal Government Office of Management and Budget (OMB) Initiatives Focused on Enhancing Sensitive Data Protection

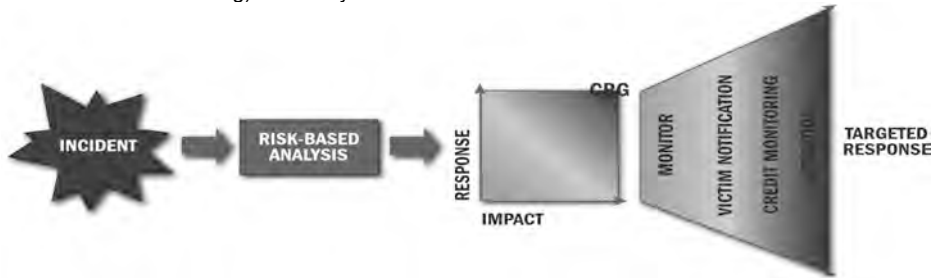


President's Identity Theft Task Force Recommendations

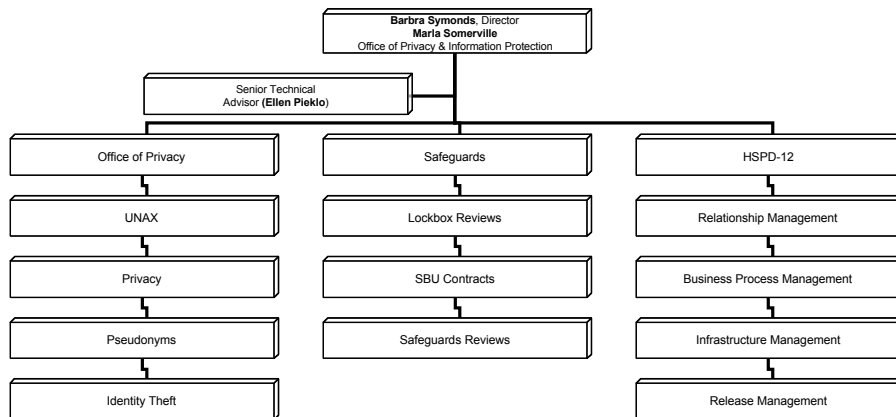


► **Key recommendations:**

1. **Identify a core response group (CRG)** to be convened upon identification of a potential data breach. CRG should include agency senior leadership such as the CIO, General Counsel, Chief Privacy Officer, and TIGTA.
2. **Develop risk-based analysis** to determine whether the incident being examined has the potential for identity theft.
3. **Implement a response plan** to identify mitigation measures (e.g. credit monitoring) and notify affected individuals of the incident.



IRS Office of Privacy & Information Protection





FedState Data Exchange Program

- ▶ Secure Tape Delivery Service
 - Special shipping and handling requirements; traceability; security containers in a tamper resistant seal
 - Ceases when encrypted electronic transmission comes online In June and July 2007
 - Shipment of tapes resumed last week
- ▶ Encrypted Electronic Transmission (EET)
 - Utilizes Tumbleweed Secure Transport product, to be provided by IRS to FedState agencies
 - Test partners are being solicited, with target to begin testing in April

21



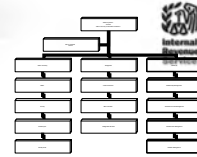
HSPD-12 Requires a Common Identification Standard for Federal Employees and Contractors

- ▶ Homeland Security Presidential Directive-12 (HSPD-12) was signed on August 27, 2004
- ▶ HSPD-12 requires the common identification card to be:
 - Secure and reliable
 - Issued based upon sound criteria for verifying an individual's identity
 - Resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation
 - Allow both physical access and logical access to Federally-controlled facilities and information systems



22

HSPD-12 Implements Security Convergence in Support of Identity Management



- ▶ Compliance with HSPD-12 is intended to:
 - Reduce inconsistent agency approaches to facility security and computer security
 - Increase the security of Federal facilities and information systems by authenticating that “you are who you say you are”
 - Enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy
 - Common identification standard to support interoperability within and between Federal departments and agencies



One System—One Credential

23

Questions?

24