



IHS Division of Information Security

IHS and HHS Security Overview

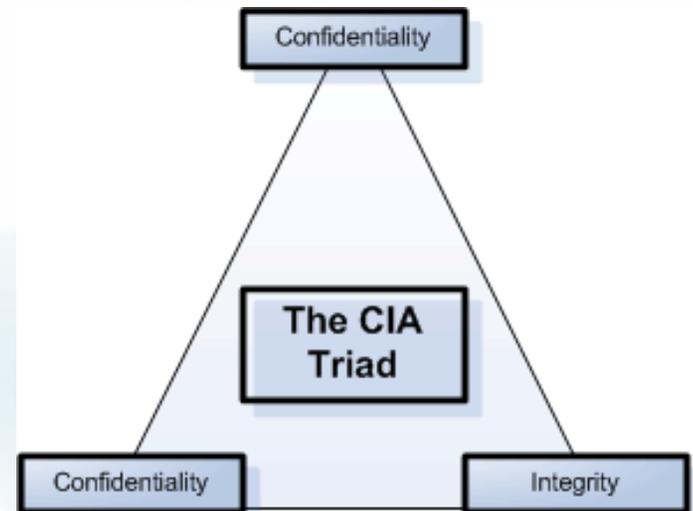
Juan Torrez - Contractor





Information Security: What's in it for me?

- Critical to IHS Mission
- FISMA requires that IHS have a sound Information Security program in place
- A robust security program provides the foundation to:
 - Preserve **confidentiality**
 - Safeguard data **integrity**
 - Provide for timely and reliable **availability** of information and systems





IHS Division of Information

SECURITY



- **IHS must break the “code of silence.”**
- IHS users must work together as a team to address cyber security issues.
- IHS must encourage collaboration.

Vigilance

Resilience





IHS Division of Information

SECURITY



ISAC Priority #10 FY 08-09

Security

- Design and provide methods and standards to assure the privacy of all patient related data that will meet or exceed HIPAA and other government security requirements.





IHS Division of Information

SECURITY



Agenda

- Data Loss
- HHS Focuses on the Data
- HHS Security Architecture Initiative
- HHS Current and Future Plans
- IHS Security Program Initiatives





Failure to support an integrated security program can have a significant impact on IHS

NEWS POLITICS OPINIONS LOCAL SPORTS ARTS & LIVING CITY GUIDE

washingtonpost.com Sign In | Register Now

The Washington Post
Print Edition | Subscribe | PostPoints

Patients' Data on Stolen Laptop

Identity Fraud Not Likely, NIH Says

By Ellen Nakashima and Rick Weiss
Washington Post Staff Writers
Monday, March 24, 2008, Page 10

A government laptop computer containing sensitive medical information on 2,500 patients

NIH not send letters notifying the affected patients of the breach until last Thursday -- almost a month later. They said they hesitated because of concerns that they would provoke a lawsuit.

“Seven years' worth of clinical trial data, including names, medical diagnoses and details of the patients' heart scans. The information was not encrypted, in violation of the government's data-security policy.”

Sign In | Register Now

boston.com

Local Search

HOME Local

HOME/NEWS

Hannaford hit with class action suit in data breach

AP Associated Press

Email | Print | Single Page | Text size

March 19, 2008

PORTLAND, Maine—Hannaford Bros. Co. already has been hit with two class action lawsuits over a data breach that exposed the names and credit and debit card numbers of thousands of customers.

A Philadelphia-based attorney filed the suit in U.S. District Court in Portland, charging the retailer with negligent security.

The firm's attorneys are forcing the retailer to pay the charges.

A similar lawsuit was filed in a federal court in Portland last week.

Carol Eleazer, Hannaford vice president of marketing, said the Scarborough-

Compromise of 4.2 million credit and debit cards.

TJX has settled many of those suits, contributing to a total of about \$250 million that the retailer has spent or set aside thus far to cover its breach-related costs.



IHS Division of Information

SECURITY



Post- NIH Incident Action Items: Encryption

- **Operating Divisions (OPDIVs) have the resources to and should:**
 - Laptops
 - Ensure all laptops are protected with Pointsec for PC and Pointsec Protector or PME
 - Ensure all new laptops are encrypted before deployment

- **HHS is currently purchasing the following resources; upon procurement, OPDIVs should:**
 - Desktops
 - Deploy Pointsec for PC to desktops that process sensitive information and may be at risk for theft
 - Deploy Pointsec Protector to all desktops (if PME is not already in place) within 30 days of procurement
 - Ensure all new desktops contain Pointsec Protector before deployment
 - Mobile Devices
 - Deploy Pointsec for Mobile Devices to all unencrypted non-Blackberry devices within 30 days of procurement
 - Ensure all Blackberry devices are encrypted in accordance with policy
 - Ensure all new devices are encrypted before deployment



IHS Division of Information

SECURITY



Post- NIH Incident Action Items: Policy

- **OPDIVs are strongly encouraged to:**
 - Distribute, track, and review *HHS Rules of Behavior (HHS Rules)* to ensure the latest version has been signed by all staff and contractors
 - Track general security awareness and role-based training
 - Participate in OPDIV-level Breach Response Team (BRT) table-top exercises to ensure preparedness in the event of a breach

Business community leaders must communicate that protecting sensitive information is a priority and that compliance is mandatory.



IHS Division of Information

SECURITY



IHS established an overarching information security program to meet legislative requirements and mitigate risk

- Almost 20,000 information system users over 12 Areas
- Attractive high profile target
 - Sensitive medical information
 - Patient information
 - Intellectual property
 - Financial and budgetary data

Terrorists, organized crime, identity theft





IHS Division of Information

SECURITY



IHS has lost its share of devices

IHS Incident Response Data 1/1/07 – present

2 desktops



9 laptops



4 PDA/blackberries



Mobile Devices
??





IHS Division of Information

SECURITY



The cost of protecting IHS PII is a fraction of the potential cost resulting from a breach

- IHS Stolen Desktop April 2007
- Contained PII
- Notification letters
- Credit monitoring



**Departmental provided PointSec
license: \$ Minimal**



IHS Division of Information



A full breach of IHS PII would cost IHS millions

IHS has 1.9 million potential patients

\$17.4 Million

Phoenix Indian Medical Center (PIMC)

52,403 patients





IHS Division of Information

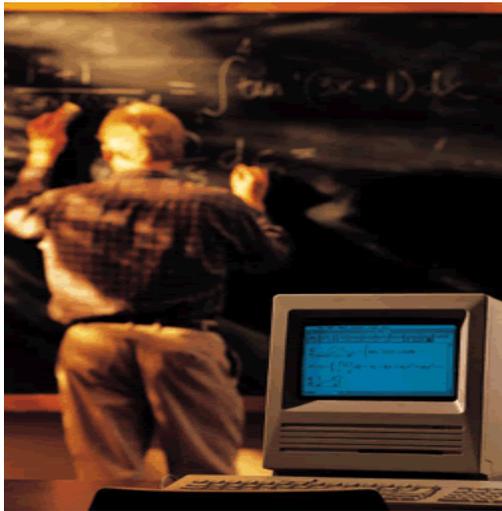
SECURITY



What can be done to prevent these potential losses?



Physical
Security
Controls



User
Education –
Store data on
Network



Encryption





IHS Division of Information

SECURITY



Agenda

- Data Loss
- HHS Focuses on the Data
- HHS Security Architecture Initiative
- HHS Current and Future Plans
- IHS Security Program Initiatives



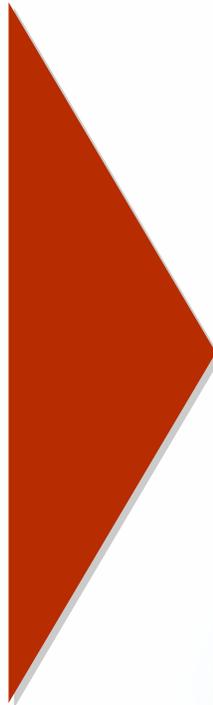


New legislative requirements and recent incidents are both driving a new approach to HHS' IT security

DRIVERS

Legislative Requirements

Incidents/Events

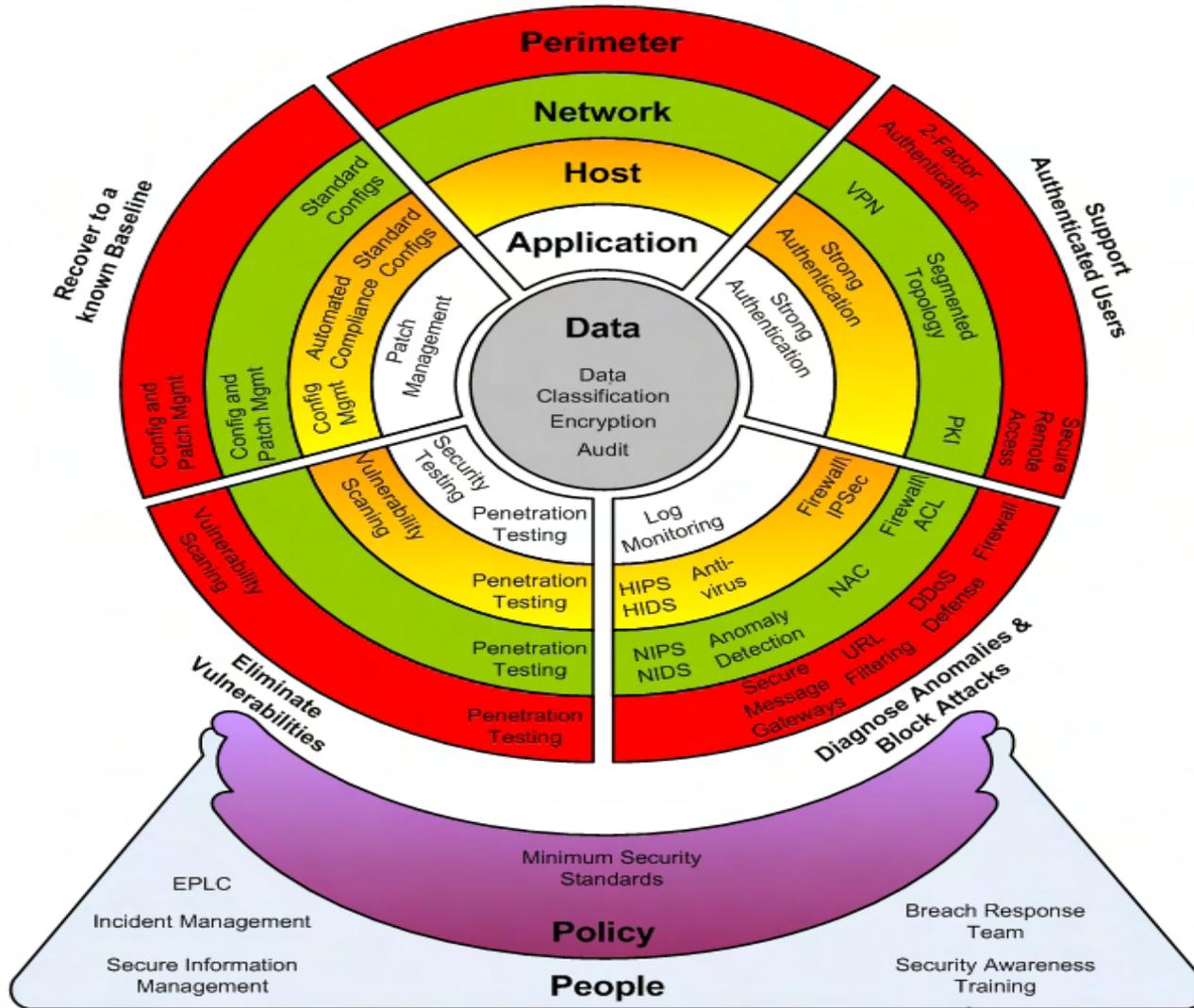


IMPACT

- Requires HHS to establish adequate policies and update existing policies
 - Requires improvements to current processes and procedures
 - Requires the implementation new tools or upgrades to current tools
-
- Requires HHS to be more prepared for a higher risk of network intrusion and physical loss of property
 - Requires the creation of new training, as well as update existing training throughout the Department
 - Requires the implementation of new tools and controls



The HHS Security Program is centered around the protection of data





IHS Division of Information

SECURITY



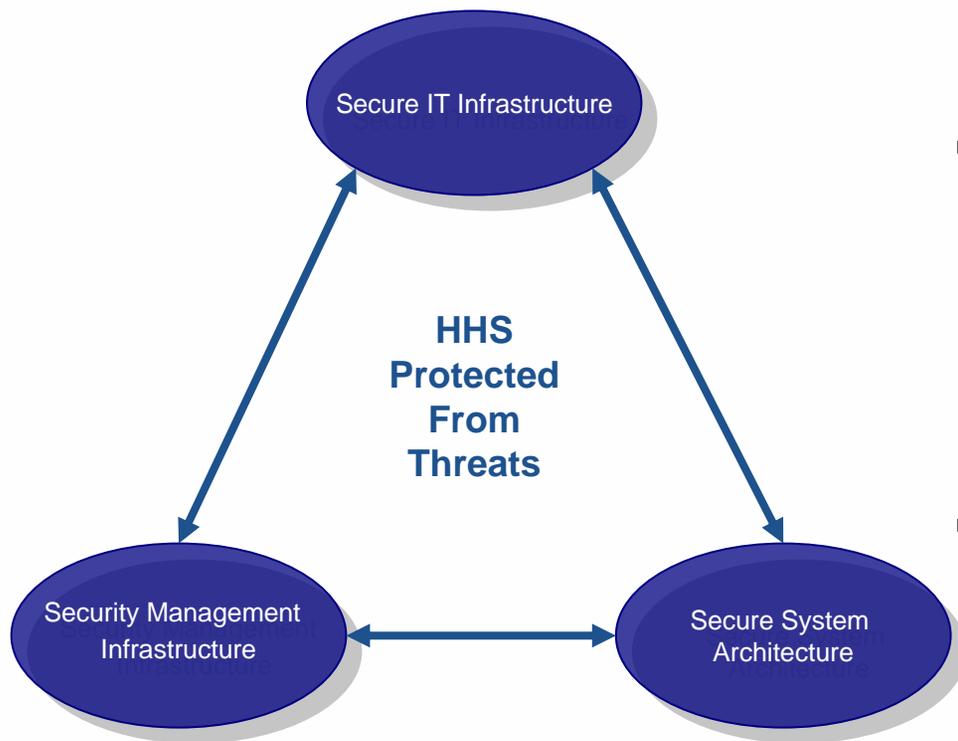
Agenda

- Data Loss
- HHS Focuses on the Data
- HHS Security Architecture Initiative
- HHS Current and Future Plans
- IHS Security Program Initiatives





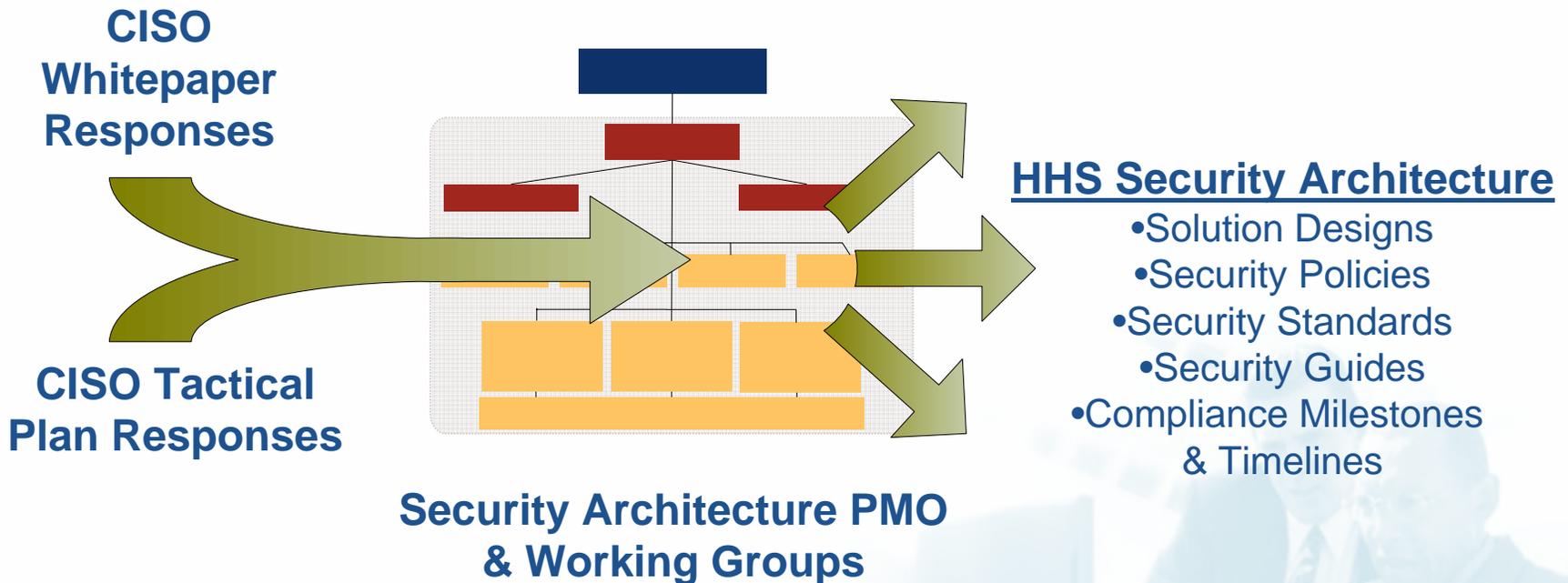
HHS' SA centers around three focus areas: **Secure IT Infrastructure**, **System Security Infrastructure**, and **Security Management Infrastructure**



- **Secure IT Infrastructure** – addresses devices that provide the underlying connectivity and communications for HHS
- **Secure Systems Architecture** – addresses the inherent untrustworthiness of all networks by providing encrypted communications and strong-authentication for all server and application access
- **Security Management Infrastructure** – integrates systems required to increase the overall security visibility, situational awareness, and coordination of security incident response at HHS



The HHS Enterprise Security Architecture Working Groups and sub-groups allow for IHS contribution to the planning and implementation of the target Security Architecture



Completed
3/15/2008

Kick-off
3/19/2008

Complete
FY '11



IHS Division of Information

SECURITY



HHS Security Architecture Status and Next Steps

■ Status

- March 6, 2008: Briefed Security Architecture plan of action and supporting tasks to OPDIV CIOs and CISOs
- March 14, 2008: Collected names of Program Management Office (PMO) and Working Group (WG) participants from OPDIV CISOs
- March 15, 2008: Received OPDIV CIO comments in response to February 20, 2008 OCIO data call
- March 19, 2008: Held PMO kick-off meeting to establish WG goals and determine next steps

■ Next Steps

- WGs will meet individually to:
 - Review current ongoing activities and determine projects that should be expanded or reduced
 - Review OCIO Security Architecture Whitepaper recommendations and identify short, mid, and long-term activities
- Full PMO will reconvene to share their review findings on April 24, 2008



IHS Division of Information

SECURITY



Agenda

- Data Loss
- HHS Focuses on the Data
- HHS Security Architecture Initiative
- HHS Current and Future Plans
- IHS Security Program Initiatives





HHS Security Architecture Tool Implementation

- Several tool implementations are making progress across the Department:

Tool	Capability	Status	Next Steps
Watchfire AppScan	<ul style="list-style-type: none"> Web-Based Application Vulnerability Detection 	<ul style="list-style-type: none"> Secure One HHS and Watchfire teams presented AppScan results and provided training to the Agency for Healthcare Research and Quality (AHRQ) on March 12, 2008 Health Resources and Services Administration (HRSA) and Indian Health Service (IHS) installations are nearing completion 	<ul style="list-style-type: none"> Schedule presentation of AppScan findings and provide training to HRSA Engage remaining OPDIVs for deployment in the next few weeks Encourage OPDIVs to remain active in implementations to ensure project remains on schedule
SecureFusion by Gideon	<ul style="list-style-type: none"> Vulnerability Management Configuration Compliance 	<ul style="list-style-type: none"> Received tool selection concurrence from majority of OPDIVs <ul style="list-style-type: none"> Received request from Centers for Medicare and Medicaid Services (CMS) for additional time to perform testing on the tool Held technical kick-off pilot at CMS on March 17, 2008 	<ul style="list-style-type: none"> Implement CMS pilot on April 3, 2008 Procure tool for Department-wide implementation



HHS Security Architecture Tool Implementation (cont'd)

Tool	Capability	Status	Next Steps
Websense	<ul style="list-style-type: none">• Website Filtering• Internet Use Policy Compliance and Auditing	<ul style="list-style-type: none">• OPDIVs approved of the Standard for Managing Outbound Internet Traffic• OPDIVs requested an opportunity to review existing filter settings across the Department before finalizing the Websense Minimum Configuration Guide	<ul style="list-style-type: none">• Lead final OPDIV review of configuration guide on April 1, 2008• Submit standard and configuration guide for formal approval• Coordinate installation timeline with Office of Information Technology Operations (OITO) and Food and Drug Administration (FDA)• Coordinate a Websense community with OPDIV technical contacts to support new installations and configuration changes



Tool Investment Update

- HHS continues to invest in various tools to strengthen the Department's security posture:

Capability	Vendor	Status	Next Steps
Incident Management and Additional Requirements	Booz Allen Hamilton	<ul style="list-style-type: none"> Started Fiscal Year 2008 (FY08) procurement process Submitted final funding paperwork; currently in the signature approval process 	<ul style="list-style-type: none"> Continue to provide HHS Computer Emergency Readiness Team (HHS-CERT), BRT, and additional requirements support
Encryption	Pointsec (PC and PME)	<ul style="list-style-type: none"> Started FY08 procurement process Submitted final funding paperwork; currently in the signature approval process 	<ul style="list-style-type: none"> Purchase and implement Pointsec licenses across OPDIVs
Vulnerability Management and Configuration Compliance	SecureFusion by Gideon	<ul style="list-style-type: none"> Developing an Acquisition Plan and Statement of Work (SOW) for the final procurement process 	<ul style="list-style-type: none"> Procure tool for Department-wide implementation



Tool Investment Update (cont'd)

Capability	Vendor	Status	Next Steps
Web-Based Application Vulnerability Detection	Watchfire AppScan	<ul style="list-style-type: none"> • Start procurement process in April 2008 	<ul style="list-style-type: none"> • Renew Watchfire contract (expires May 15, 2008)
Website Filtering and Internet Use Compliance and Auditing	Websense	<ul style="list-style-type: none"> • Purchased 81,000 licenses on December 20, 2007, which include: <ul style="list-style-type: none"> . AHRQ - 750 . Centers for Disease Control and Prevention (CDC) - 14,000 . HRSA - 2,000 . IHS - 15,000 . NIH - 30,250 . Program Support Center (PSC) - 1,500 	<ul style="list-style-type: none"> • Purchase 2,500 additional licenses



IHS Division of Information

SECURITY



Agenda

- Data Loss
- HHS Focuses on the Data
- HHS Security Architecture Initiative
- HHS Current and Future Plans
- IHS Security Program Initiatives





IHS Division of Information

SECURITY



Network Monitoring

US-CERT Einstein

SECURIFY™



NOSC - Cisco IDS



Future Network Monitoring Projects

- Stand alone Nessus devices to be deployed throughout IHS
- Implemented and administered by OIT
- Can be used for Ad-Hoc scanning
- Feed into our vulnerability management program





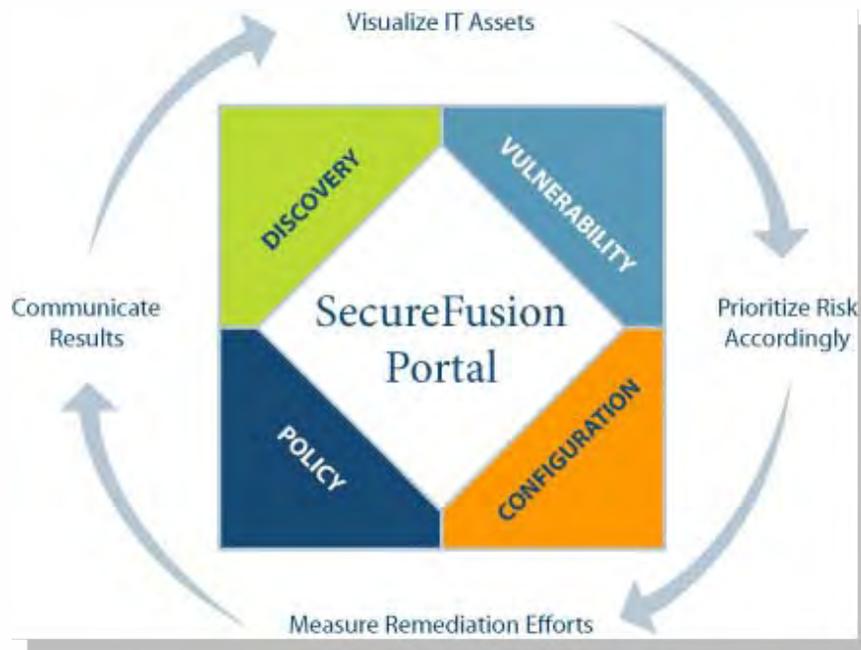
Future Vulnerability Management

- Vulnerability and Configuration Management requirements are derived from the OMB mandate and the current NIH Vulnerability Scanning Program:



GIDEON TECHNOLOGIES

Know your assets. Know your risk.



- **Asset Discovery**
- **Vulnerability Management**
- **Compliance Management**
- **Reporting and Updating**
- **Security Controls**
- **Pros:**
 - SCAP compliance for FDCC scanning
 - Tracking and host matching ability
 - Inventory and statistical reporting capability
 - Ease of use (Intuitive web console to navigate and configure)
 - Scheduling
 - SQL backend



IHS Division of Information

SECURITY



RPMS Server Hardening and Config Mgt

- Standards for hardening RPMS servers (both AIX and Windows)
- Standards for change management
- Procedures for server maintenance
- Auditing Standards





IHS Division of Information

SECURITY



The PointSec Mandate

HHS MEMORANDUM ISP-2006-009

To support this recommendation, the Department of Health and Human Services (HHS) has purchased PointSec for PC with Media Encryption (Pointsec) from Pointsec Technologies for implementation by OPDIVs. OPDIVs are required to implement Pointsec, or a Federal Information Processing Standard (FIPS) 140-2 compliant whole disk encryption product, on all laptop computers no later than March 31, 2007



PointSec

Enforceable Security

Automatic, full disk encryption – No user intervention

Complete Solution

Covers Laptop/PC, Management, Remote Access, Symbian, Smartphone, Pocket PC & Palm

Quick & Easy To Administer

No significant overhead

Password Reset

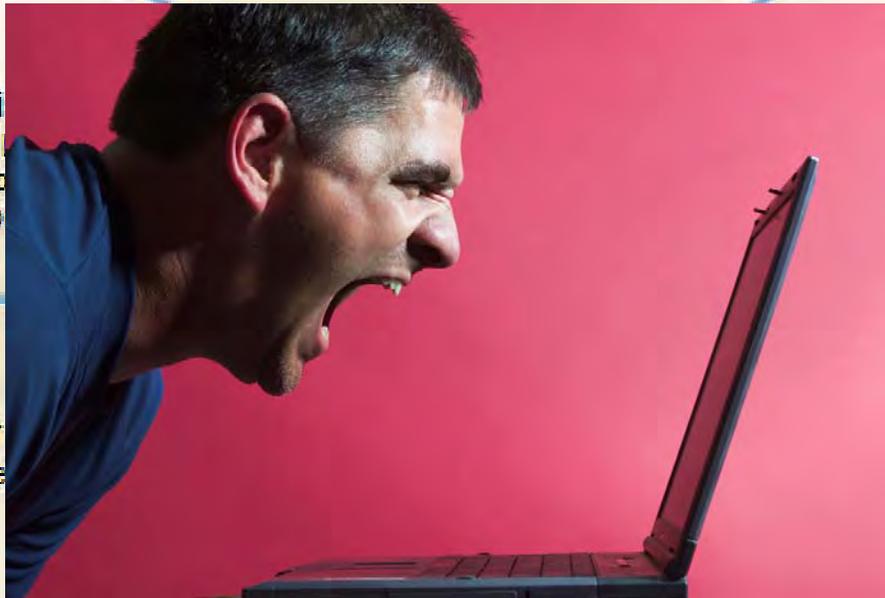
challenge / response

Reduced Device Costs

disk wipe/conditioning

Exposure From Lost Data Eliminated

Only replacement cost for device





PointSec Media Solution

HHS Standard 2007-0001.001S

- (2) All mobile devices (including non-HHS laptops) and portable media that contain sensitive agency data shall be encrypted using a FIPS 140-2 compliant product, effective 180 days from approval of this standard. -- Signed Aug. 21, 2007
- What does it do?
 - Encrypts documents added to - USB Keys; CDs; Floppies; and external Hard Drives
 - HHS purchased enough licenses to cover entire IHS inventory
 - Had sessions with all Area Offices to give access and go over software
 - Email issues – SecureZip, WinZip, PKI Certificates



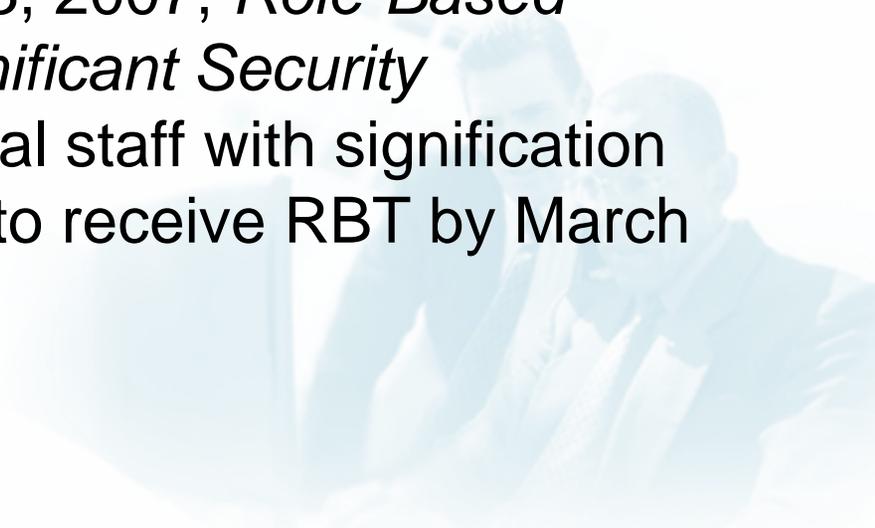
IHS Division of Information

SECURITY



IHS is currently at 78% compliance for role-based training

- Role-based training is specialized training for those with significant IT security roles and responsibilities which is relevant to their role.
- Memorandum issued October 3, 2007, *Role-Based Training of Personnel with Significant Security Responsibilities*, requires federal staff with significant security responsibilities (SSR) to receive RBT by March 31, 2008





IHS is well on its way to 100% compliance for annual security awareness FY08

Area Counts						
Area	Facilities	Register	Passed	Failed	In Progress	Accepted
<u>Aberdeen</u>	92 / 37	<u>2416</u>	<u>2052</u>	0	<u>364</u>	<u>2052</u>
<u>Alaska</u>	315 / 276	<u>17</u>	<u>9</u>	0	<u>8</u>	<u>9</u>
<u>Albuquerque</u>	89 / 89	<u>1870</u>	<u>1574</u>	0	<u>296</u>	<u>1572</u>
<u>Bemidji</u>	406 / 120	<u>703</u>	<u>686</u>	0	<u>17</u>	<u>686</u>
<u>Billings</u>	76 / 36	<u>1459</u>	<u>1296</u>	0	<u>163</u>	<u>1295</u>
<u>California</u>	182 / 132	<u>1504</u>	<u>1211</u>	0	<u>293</u>	<u>1210</u>
<u>Nashville</u>	83 / 83	<u>163</u>	<u>141</u>	0	<u>22</u>	<u>141</u>
<u>Navajo</u>	213 / 65	<u>5010</u>	<u>4217</u>	0	<u>793</u>	<u>4214</u>
<u>Oklahoma</u>	134 / 134	<u>2256</u>	<u>2066</u>	0	<u>190</u>	<u>2065</u>
<u>Phoenix</u>	187 / 106	<u>3210</u>	<u>2754</u>	0	<u>456</u>	<u>2754</u>
<u>Portland</u>	191 / 191	<u>798</u>	<u>681</u>	0	<u>117</u>	<u>681</u>
<u>Tucson</u>	63 / 63	<u>353</u>	<u>257</u>	0	<u>96</u>	<u>257</u>
<u>Headquarters</u>	4 / 3	<u>381</u>	<u>331</u>	0	<u>50</u>	<u>331</u>
<u>NP/OIT</u>	4 / 1	<u>186</u>	<u>161</u>	0	<u>25</u>	<u>160</u>
Totals	2039 / 2098	20326	17436	0	2890	17427





The online ITAC is getting close

INFORMATION Technology Division of Information

ITAC TECHNOL RESOURCES

Return original form to approving supervisor for storage.

INFORMATION TECHNOLOGY ACCESS CONTROL (ITAC) FORM

NOTE: All the following information must be provided before information system access will be granted. A copy of the Rules of Behavior shall be provided to each employee requesting access. Please submit form to the appropriate supervisor in accordance with local procedure. Please print legibly. User will fill out this form with their supervisor's assistance.

Requestor Information			
First Name	MI	Last Name	Job Title
Phone Number		E-mail Address (if known)	
Affiliation <input type="checkbox"/> IHS Employee <input type="checkbox"/> Tribal Employee <input type="checkbox"/> Commissioned Corp <input type="checkbox"/> Contractor (company: _____ date contract expires: _____)			
Type of employment <input type="checkbox"/> Full Time <input type="checkbox"/> Part Time wk hrs: _____ Time Zone: _____ <input type="checkbox"/> Temporary (Term Date: _____) <input type="checkbox"/> Volunteer			
Area/Site Information			
Area	Facility	Department	

1. An IHS Web Login.

If you have an IHS Web Systems Login (username and password), you can login by clicking the 'Login' button (left). If you do not have an IHS Web Systems Login, you can register with the system by clicking the 'Register' button (left).

ITAC Home | New Access | Update Access | Remove Access | Drafts | Annual Access Review | Team Management | Request Tracking



IHS Division of Information

SECURITY



The IHS waiver process

- I cannot comply with a particular policy or standard; how can I obtain a waiver?
- In cases in which an Area cannot comply with a policy or standard for technical or financial reasons, or because it precludes the Area from supporting its mission or business function, a justification for the non-compliance shall be documented using the *Departmental Security Policy and Standard Waiver Form*. This waiver form should be submitted to the OPDIV's appropriate security representative for approval (see form for further details). The waiver form can be found at [http://security.ihs.gov/Forms/F06-11i IS PolicyWaiver.pdf](http://security.ihs.gov/Forms/F06-11i_IS_PolicyWaiver.pdf) .



Questions?

Information Security Team: OITSecurity@ihs.gov

IHS Information Security Web site: <http://security.ihs.gov>

Contact: Kathleen Federico, Acting CISO: 505-248-4381 (Cell 505-975-4230)
Kathleen.Federico@IHS.gov

Juan Torrez (Contractor), Management Analyst: 505-248-4419 Juan.Torrez@ihs.gov