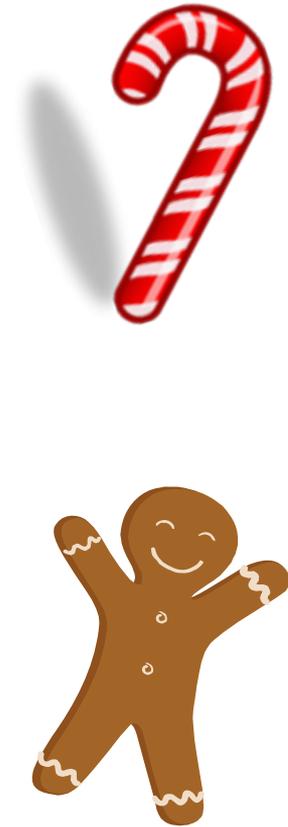




Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

December 9, 2009

December





ISOAG December 2009 Agenda

- | | | |
|-------------|---|----------------------------|
| I. | Welcome & Opening Remarks | John Green, VITA |
| II. | Defense Criminal Investigative Service Cyber Program | John Simbulan, DCIS |
| III. | Metadata: How to Leak Data Without Even Trying | Ed Miller, DOA |
| IV. | Enterprise Server Lifecycle Process | Eric Taylor, NG |
| V. | Partnership Update | Don Kendrick, VITA |
| VI. | Upcoming Events and Other Business | John Green, VITA |



Introducing

Program Security Officer

Craig Drain

Northrop Grumman

Craig.Drain@ngc.com



Defense Criminal Investigative Service

Guest Speaker

John Simbulan, SA
OIG DoD, DCIS





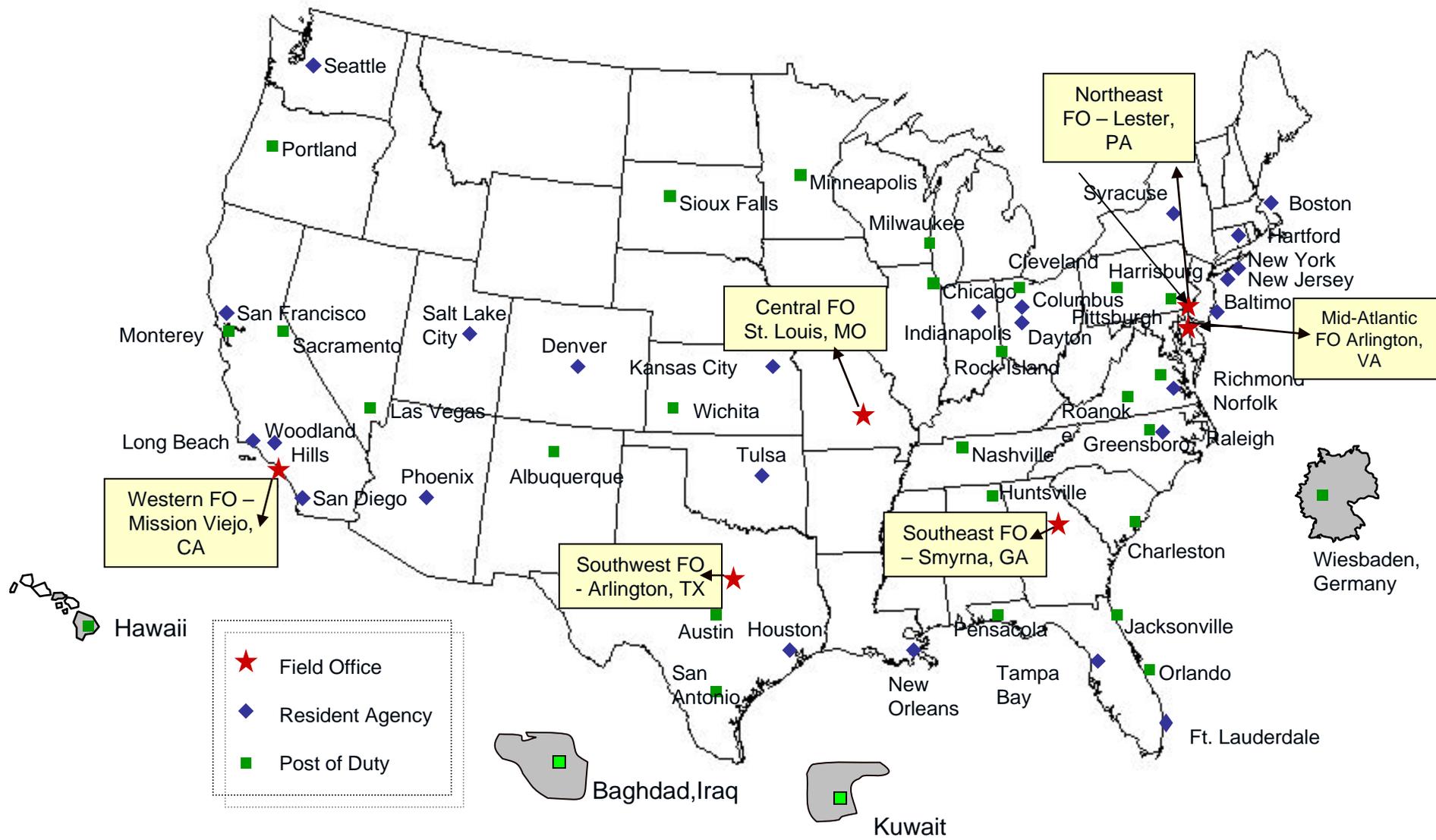
DCIS Mission

- **DCIS is the Law Enforcement Agent of the DoD-IG.**
 - Investigates allegations of criminal violations under Title 10 and Title 18, and other Federal statutes
 - Derives authority from:
 - IG Act of 1978 as amended
 - Title 10 USC Sections 1585 and 1585a
 - DoD Directive 5106.1.
- **Protect America's Warfighters.**
 - Conducting investigations in support of crucial National Defense priorities.





DCIS Office Locations





DCIS Investigative Priorities

- Terrorism
- Computer/Cyber Crimes
- Illegal Technology
Transfer/Technology Protection
- Industrial Espionage
- Fraud
- Public Corruption

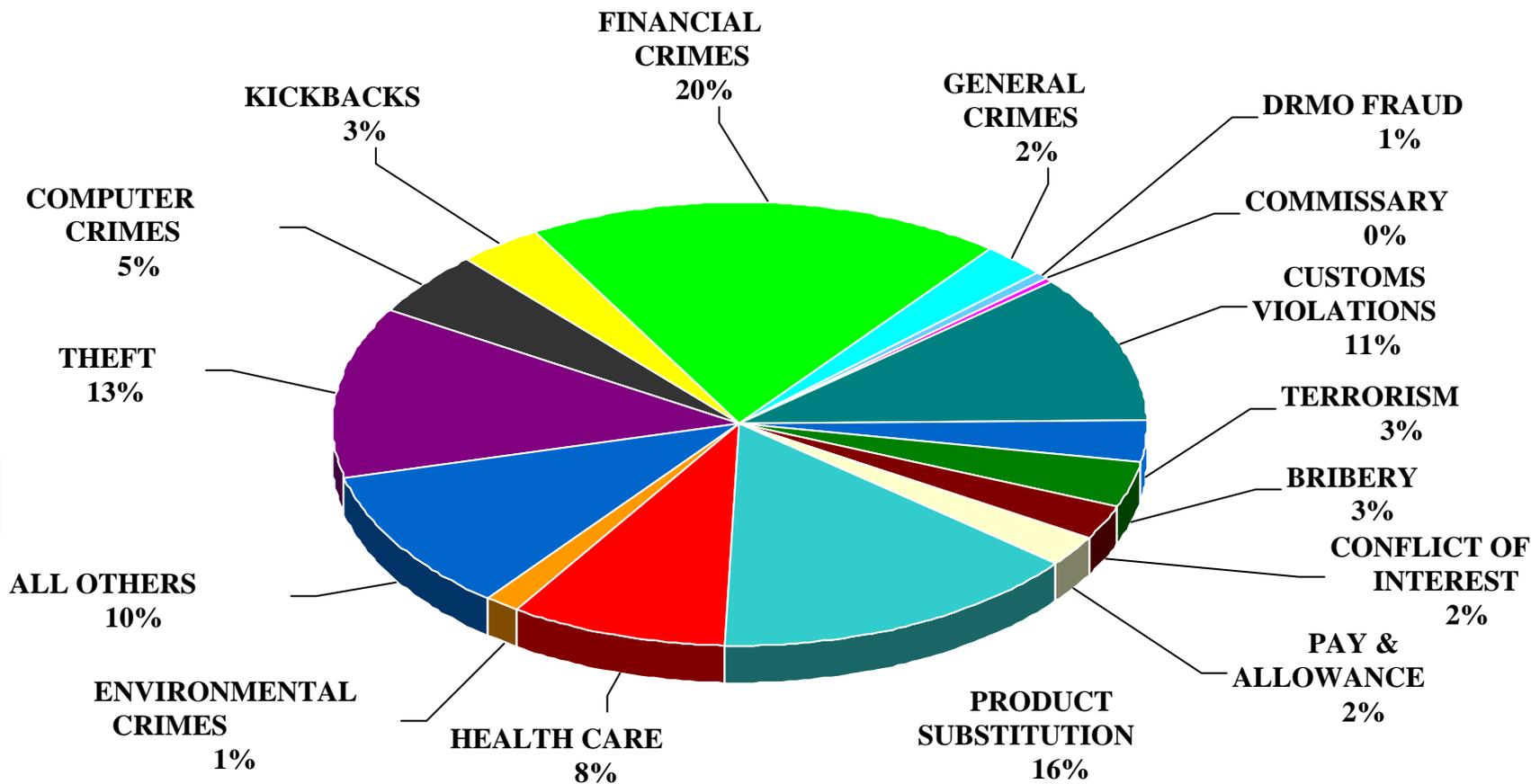


DCIS Investigative Jurisdiction

- Title 10, Title 18, and other Federal Statutes
- Office of Secretary of Defense
- Joint Chiefs of Staff
- DoD Agencies
- Combatant Commands
- Multi-Service Investigations
- Any activity with a DoD-IG Interest
 - Computer/Cyber Crime Emphasis:
Defense Contractors



DCIS Active Investigations





DCIS Computer Crime Investigations

- Computer Intrusions
- Child Exploitation (Refer Out...)
- Misuse of Government Computers
- Wiretap Statutes Violations
- Identity Theft



Computer Intrusions

All Computer Intrusions, by definition, are violations of 18 USC 1030 (Criminal Statute)

- Unauthorized Access
- Exceeding Authorized Access
- DoD Category **(CAT)** 1–8 Intrusion Incidents
- BotNets
- Malware/Adware



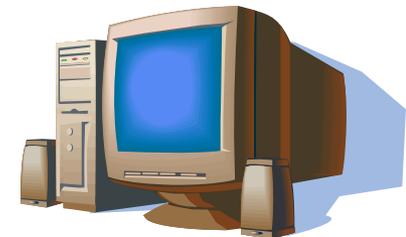


DoD Network Intrusion CAT Levels defined:

HIGH Security Risk

- CAT 1** - Full Root Access
- CAT 2** - User Level and Web Page Hacks
- CAT 3** - Attempted Access
- CAT 4** - Denial of Service
- CAT 5** - Poor Security Practice
- CAT 6** - Probes/Scans
- CAT 7** - Malicious Logic
- CAT 8** - Unconfirmed

Low Security Risk





Computer Intrusions-DoD Contractor Sites

- Increase incidents of Computer Intrusions on DoD Contractor Sites.
- Significant loss of data and trade secrets of National Security Programs (USN, USMC, Army, USAF)
 - Aerospace
 - Precision Sensors & Components
 - Missiles & Munitions



Computer Intrusions-DoD Contractor Sites

Damage Assessment

1. Background of Attack:
 - A. Server was compromised via a known vulnerability.
 - B. Compromised Server was used as a launch pad for subsequent attacks against other internal hosts.
 - Over 40 Hosts enterprise-wide were compromised
 - Perpetrators compressed and moved data to centralized repositories within VICTIM network. Data was then transported to unauthorized foreign hosts.
 - Final destination of data remains unknown.



Computer Intrusions-DoD Contractor Sites *Damage Assessment*

2. Compromise of Export Controlled Technical Data:
 - A. PROGRAM Specific
 - B. PRODUCT Specific
 - C. COMMERCIAL Oriented

3. Technical Data Loss Defined:
 - A. Customer Specification and design review data
 - B. Detailed Design Data
 - C. Software Source Code
 - D. Design plans for next generation product lines



Computer Intrusions-DoD Contractor Sites

Damage Assessment

4. Network Environment Issues:
 - A. 100's of External Points of Presence
 - Network Gateways
 - Data Centers
 - B. Multiple Network Infrastructure Models
 - C. Unclear Cross Ownership of Domain Groups / Undefined Security Policies, Un-centralized Network Operations Center
 - D. Undefined Incident Response Reporting Procedures



Defense Contractors

1. EDUCATE:

A. Increase contractor awareness of domestic and foreign national security threats.

- ✓ Insider Threats: Identify personnel that possess knowledge and unique access
- ✓ Outsider Threats: Understand the threat posed by foreign intelligence services and economic competitors



Defense Contractors

2. INCIDENT RESPONSE - PROACTIVE ATTACK DETECTION:

- A. Establish response team(s):
 - ✓ Global Alert Monitoring, Crisis Response Team(s), Incident Response Team(s).
- B. Ensure Continuity of Operations, while Implementing countermeasures to prevent further collection or damage.
- C. Implement Incident response and proactive reporting that will enable key partnerships with Law Enforcement to assist and mitigate.



Defense Contractors

3. ASSESS AND IMPLEMENT:

- A. Increase **INFORMATION ASSURANCE** best practices
- B. Identify, assign value, and limit access to industry trade secrets:
 - ✓ Financial/Economic resources
 - ✓ Scientific, Engineering, and Technical prototypes, designs, and tests.
- C. Enterprise-Wide Incident Response Reporting Procedures.



Defense Contractors

4. **ESTABLISH KEY PARTNERSHIPS:**

- A. Effective incident response reporting depend on effective collaboration:
 - ✓ Internal Partnerships – First Responders, Network Ops Centers, Enterprise Policy, and Management
 - ✓ External Partnerships – Law Enforcement and U.S. Intel Communities
- B. Defined Information sharing system within formal security policies.
 - ✓ What should be reported
 - ✓ How should it be reported
 - ✓ Who should it be reported to



DCIS Incident Response

- Identification of Incident and Victim
- Contact Victim
 - Identify & Preserve Evidence
 - Obtain Volatile Data, Hard Drive Image(s) & Logs
 - Gather Background Data & Damages
 - Identify Perpetrator(s)
- Pursue Criminal Leads and/or Monitoring:
 - Ensure **CONFIDENTIALITY** Reporting
 - Intelligence / Criminal Reporting
 - Recommend countermeasures



DCIS Partnerships

- United States Attorney
- FBI Cyber Crime Task Force
- USSS Electronic Crimes Task Force
- JTF-GNO LECIC
- NSA/NTOC
- US Army CID CCIU
- Naval Criminal Investigative Svc. Cyber Division
- Air Force Office of Special Investigations
- Counter Intelligence Field Activity (CIFA)
- ASD(NII) & DUSD(CI&S)



DCIS High Tech Crime Team

Mid-Atlantic Field Office

Computer Crimes Coordinator

Special Agent Jeffery Thorpe

Jeffery.Thorpe@dodig.mil

High Tech Crime Team

Special Agent John Simbulan

John.Simbultan@dodig.mil

W: (703) 604-8448 Cell: (703) 299-2513



*WHO IS RESPONSIBLE FOR THE
SECURITY OF OUR NETWORKS?*

*ISN'T THERE A LAW OR POLICY THAT
REQUIRES US TO SECURE OUR
NETWORKS?*

***INFORMATION IN THE FOLLOWING SLIDES WERE OBTAINED FROM THE
DEFENSE INFORMATION SYSTEMS AGENCY FACILITY SECURITY OFFICE***



WHY INFORMATION ASSURANCE

- ❑ Required by law, Executive Branch, and DoD policy

- ❑ Information Assurance is defined as: “Measures that protect and defend information and information systems by ENSURING their **C**onfidentiality, **I**ntegrity, **A**vailability, , authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.”
[Committee on National Security Systems (CNSS) Instruction # 4009]

- ❑ Congress enacted legislation in response to issues with regard to information system and computer security. Since terrorist attacks of 9-11, defense of the U.S. information infrastructure has been a Congressional Priority.



Legislative Concerns

- Congress desired:
 - Export Licenses for critical or sensitive information technology
 - Communication Safeguards
 - National Security Information Protection
 - Prohibit unauthorized/fraudulent access
 - Ensure minimum protection in multi-user environment
 - Privacy
 - Safeguard personal Data, provide notification when personal information collected
 - Prevent unauthorized interception of communications.



Legal

- Computer Fraud and Abuse Act
 - Signed into law in 1986; prohibits unauthorized or fraudulent access to government computer systems
 - Maximum fine of up to \$5,000 or double the value of anything obtained via the unauthorized access, plus up to 5 years imprisonment. (Robert Morris Jr., author of the internet worm, was the first person convicted under this law)



Legal

- Computer Fraud and Abuse Act (*Continued*)
 - Included in Title 18, U.S. Code
 - Possession of illegal Access Devices (18 USC 1029)
 - Unauthorized Access to Gov Systems (18 USC 1030)
 - Crime committed when entering system to:
 - Acquire national defense information
 - Obtain financial information
 - Deny the use of the computer
 - Commit Fraud



Federal Information Security Management Act (FISMA)

- Replaced the Computer Security Act of 1987
- Included at Title III, of the E-Government Act of 2002, Signed into law 12/17/2002.
- Expounded on requirement Agencies report to congress
 - Requires for both Unclass and National Security Programs to perform:
 - Annual Agency program reviews
 - Annual Inspector General (IG) evaluations
 - Agency reporting to Office of Management Budget (OMB)
 - Results of IG evaluations for unclassified systems
 - Audits of IG evaluations for national security programs
 - An annual OMB report to Congress



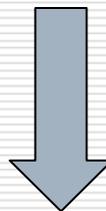
Federal Information Security Management Act (FISMA) ...*Continued*

- Required Agencies to identify risk levels associated with their systems and implement the appropriate level of protections accordingly
- Strengthened the role played by the National Institute for Standards and Technology (NIST) in developing and maintaining standards and guidelines for minimum information security controls

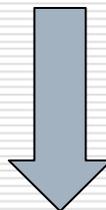


Security Policy Hierarchy

Congressional Law



National Security Policy & Directives



DoD Policy, Directives, & Instructions



DoD Security Policy

<u><i>Publication Examples</i></u>	<u><i>Origin of Development</i></u>	<u><i>Type of Publication</i></u>
Regulations Instructions, & Manuals	USAF, Army, Navy, USMC	Joint Command, Service, and Agency-Specific Policy & Directives
	DoD	Policies and Directives
Common Criteria, FIPS Pubs, Rainbow Book Series	NSA, NIST, CNSS, NCSC, DHS	Guidelines, Pubs, Standards
Presidential Directives, OMB Circulars, National Security Decision Directives (NSDD), Presidential Decision Directives (PDD), Homeland Security Directive (HSPD)	Executive Branch	Federal Gov-Wide Policies
Congressional Acts	Congress	Public Law



Information Assurance Policies

- OMB Circular A-130 (Management of federal Information Resources)
 - Establishes Federal Policy
 - Appendix III, Requires:
 - Information Security Plans
 - Computer Security Status Reports
 - Computer Security Awareness and Training
 - Agencies improve contingency planning
 - Formal Emergency response capabilities
 - Directs NIST, NSA, and others to develop further specific guidance
 - Describes the responsibilities of the Federal Designating Approving Authority (DAA)
 - Responsibility for security of each information system shall be assigned to a management official knowledgeable in the nature of the information and process supported by the application and in the management personnel, operational and technical controls used to protect it.



Information Assurance in DoD

- DoD Directive 8500.01E, "Information Assurance" ..dated Oct. 24, 2002.
 - Establishes Policy and assigns responsibilities to achieve DoD IA
 - Directs IA to be achieved through a defense-in-depth approach, layering both technical and non-technical solutions
 - Specifies the integration of the capabilities of personnel, operations, and technology



Information Assurance in DoD

- DoD Directive 8500 Series
 - DoDD 8500.01E and DoDI 8500.2 provide overarching IA guidance and implementing instructions.
 - DoDI 8510.01 – Certification & Accreditation
 - DoD 8520 Series – PKI, PK-Enabling, and biometrics
 - DoD 8530 Series – computer network defense (CND) and vulnerability management (IAVA, etc.)
 - DoD 8540 Series – interconnection and data transfer between security domains to include Cross Domain Solutions



Information Assurance in DoD

- ❑ DoD Directive 8500 Series
 - **DoDD 8500.01E** and **DoDI 8500.2** provide overarching IA guidance and implementing instructions.
 - ❑ Promulgate awareness that DoDD 8500.01E mandates all DoD Information Systems be Certified and Accredited (C&A)
 - ❑ ...and must: Demonstrate the security issues through the DoD Information System Certification and Accreditation Process (**DIACAP**)
 - ❑ **DITSCAP was updated and replaced by the DIACAP**



DIACAP Establishes.....

- ❑ The standard DoD Information Assurance C&A process for authorizing the operation of DoD information system(s)
- ❑ A process to manage IA capabilities and services
- ❑ An enterprise process to C&A DoD systems by implementing and managing IA capabilities described as **IA CONTROLS**
- ❑ Identify Baseline Security requirements
- ❑ Accomplish through a DoD wide configuration control and management (CCM) process that considers risk assessments



DIACAP “must be implemented”

- ❑ Federal Information Security Management Act (**FISMA**)
- ❑ **DoDD 8100.1**, Global Information Grid (GIG) – Overarching Policy
- ❑ **DoDD 8500.01E**, Information Assurance
- ❑ **DoDI 8500.2**, Information Assurance Implementation



Department Head(s) is Responsible to implement DIACAP

- The Heads of DoD Components must:
 - Ensure the DIACAP is implemented and all information systems under their purview are in compliance with the DIACAP
 - Operate only accredited information systems
 - Comply with Accreditation decisions and enforce termination dates
 - Appoint Designating Approving Authorities (DAA) for all systems under their purview
 - Provide training and ensure IA professional certification requirements are met
 - Ensure user representatives (UR) are appointed
 - Appoints a SIAO if the component has no CIO



“DIACAP Knowledge Service” resource site (www.disa.mil)

- ❑ The official DoD resource for implementing and executing the DIACAP (the DIACAP manual)
- ❑ Includes tools, diagrams, templates, process maps, IA CONTROL validation procedures, and other information to aid in the execution of the DIACAP activities such as:
 - Initiating and Planning IA C&A
 - Implementing and validating assigned IA CONTROLS
 - Making certification determinations and accreditation decisions
 - Maintaining authorizations to operate and conducting reviews
 - Decommissioning



DIACAP has

- ❑ Extensive paperwork package
- ❑ Principle Approving Authorities (PAA) and Designating Approving Authorities (DAA)
- ❑ Information Assurance Manager (IAM)
- ❑ Certification Agent (CA), CA Reps, analysts, and validators
- ❑ Defined Security Requirements driven by **IA CONTROL** validation procedures, and other information to aid in the execution of the DIACAP



DIACAP Scorecard

- ❑ Conveys information about the IA posture of a DoD information system in a format that is easily understood by readers and formatted for electronic data exchange. The IA posture is described through detailed status of the **IA CONTROLS** that have been applied to the DoD information system



Certification and Accreditation Determination / Decision

- ❑ There are 4 possible accreditation decisions:
 - **Authorization to Operate (ATO)**
 - ❑ System Meets all IA CONTROLS and has been validated
 - **Interim Authorization to Operate (IATO)**
 - ❑ System has not fully Implemented all IA controls but has a completed POA&M detailing how it will overcome the lacking security requirements which prevented ATO
 - **Interim Authorization to Test (IATT)**
 - ❑ System is in "Beta" but does not process actual DoD mission or business related data – will also have a POA&M detailing how it will meet all IA CONTROLS
 - **Denial of Authorization to Operate (DATO)**
 - ❑ System has not met specific IA CONTROLS or requirements necessary to operate securely



Latest Requirement to protect DoD information and DoD systems on NON-GOVERNMENT FACILITIES

- Assistant Secretary of Defense, Memo Dated July 31, 2009

Purpose.

In accordance with the authority in DoD Directive 5144.1 (Reference (a)), this DTM establishes policy for managing the security of unclassified DoD information on non-DoD information systems. Subchapter III of chapter 35 of title 44, United States Code (Reference (b)) mandates that DoD information and DoD information systems be appropriately protected. DoD Instruction 8510.01 (Reference (c)) addresses the protection of classified and unclassified DoD information on information systems owned by the Department of Defense or operated on behalf of the Department by non-DoD entities. DoD Manual 5220.22-M (Reference (d)) addresses the protection of classified information released or disclosed to industry, including what is processed on their information systems. This DTM is effective immediately; it shall be incorporated into the appropriate DoD 8500 series issuances within 180 days.

- All unclassified DoD information in the possession or control of non-DoD entities on non-DoD information systems, to the extent provided by the applicable contract, grant, or other legal agreement or understanding with the Department of Defense.
-



INFORMATION ASSURANCE IS NOT A
LUXURY, IT'S A LAW.....

LET'S DO OUR BEST TO DO BEST
PRACTICES AND SECURE OUR
NETWORKS !

Metadata: How to Leak Data Without Even Trying

Ed Miller

Virginia Department of Accounts



Virginia Department of Accounts

Financial Accountability. Reporting Excellence.

Chronology of Data Breaches

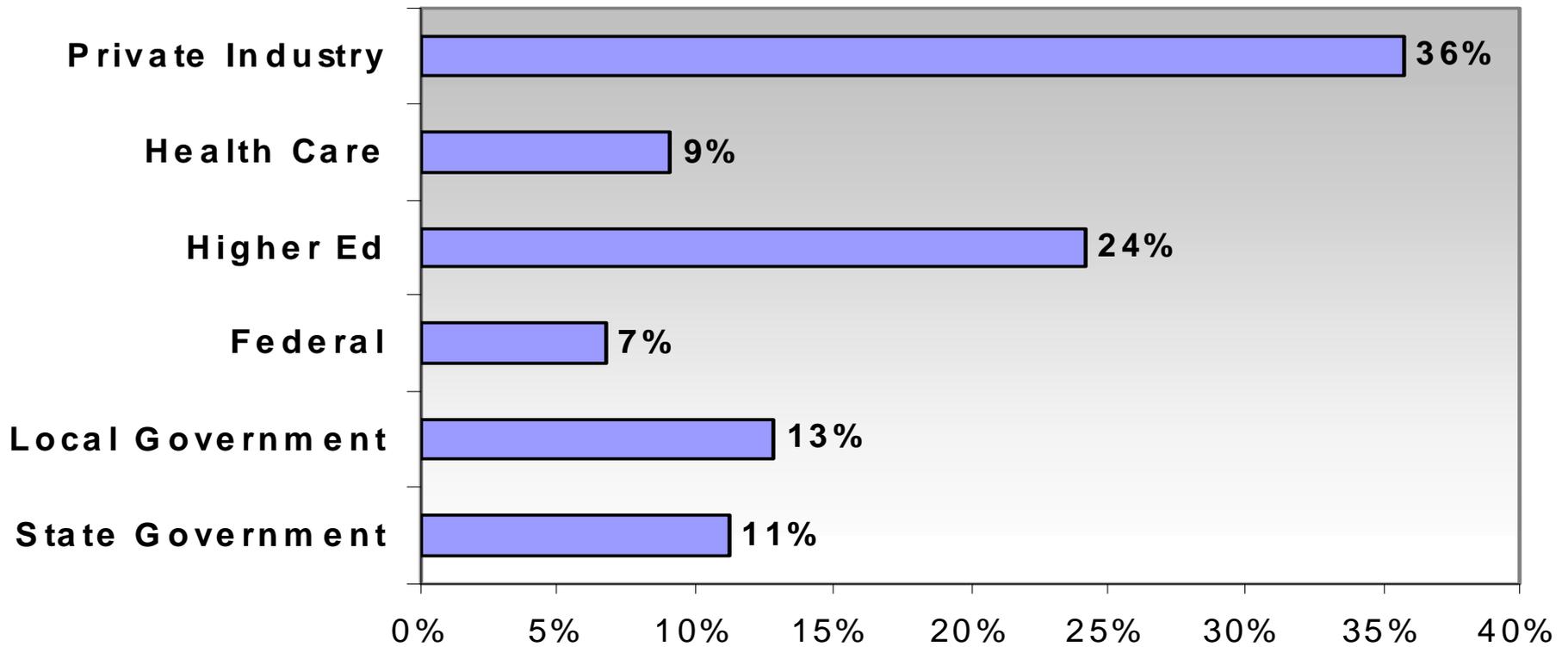
Go to Breaches for 2005, 2006, 2007, 2008 or 2009

www.privacyrights.org

DATE MADE PUBLIC	NAME(Location)	TYPE OF BREACH	NUMBER OF RECORDS
2005			
Jan. 10, 2005	George Mason University (Fairfax, VA)	Names, photos, and Social Security numbers of 32,000 students and staff were compromised because of a hacker attack on the university's main ID server.	32,000
Jan. 18, 2005	Univ. of CA, San Diego (San Diego, CA)	A hacker breached the security of two University computers that stored the Social Security numbers and names of students and alumni of UCSD Extension.	3,500
Jan. 22, 2005	University of Northern Colorado (Greeley, CO)	A hard drive was apparently stolen. It contained information on current and former University employees and their beneficiaries -- name, date of birth, SSN, address, bank account and routing number..	30,000
Feb. 12, 2005	Science Applications International Corp. (SAIC) (San Diego, CA)	On Jan. 25 thieves broke into a SAIC facility and stole computers containing names, SSNs, and other personal information of past and	45,000 employees

Industry Analysis

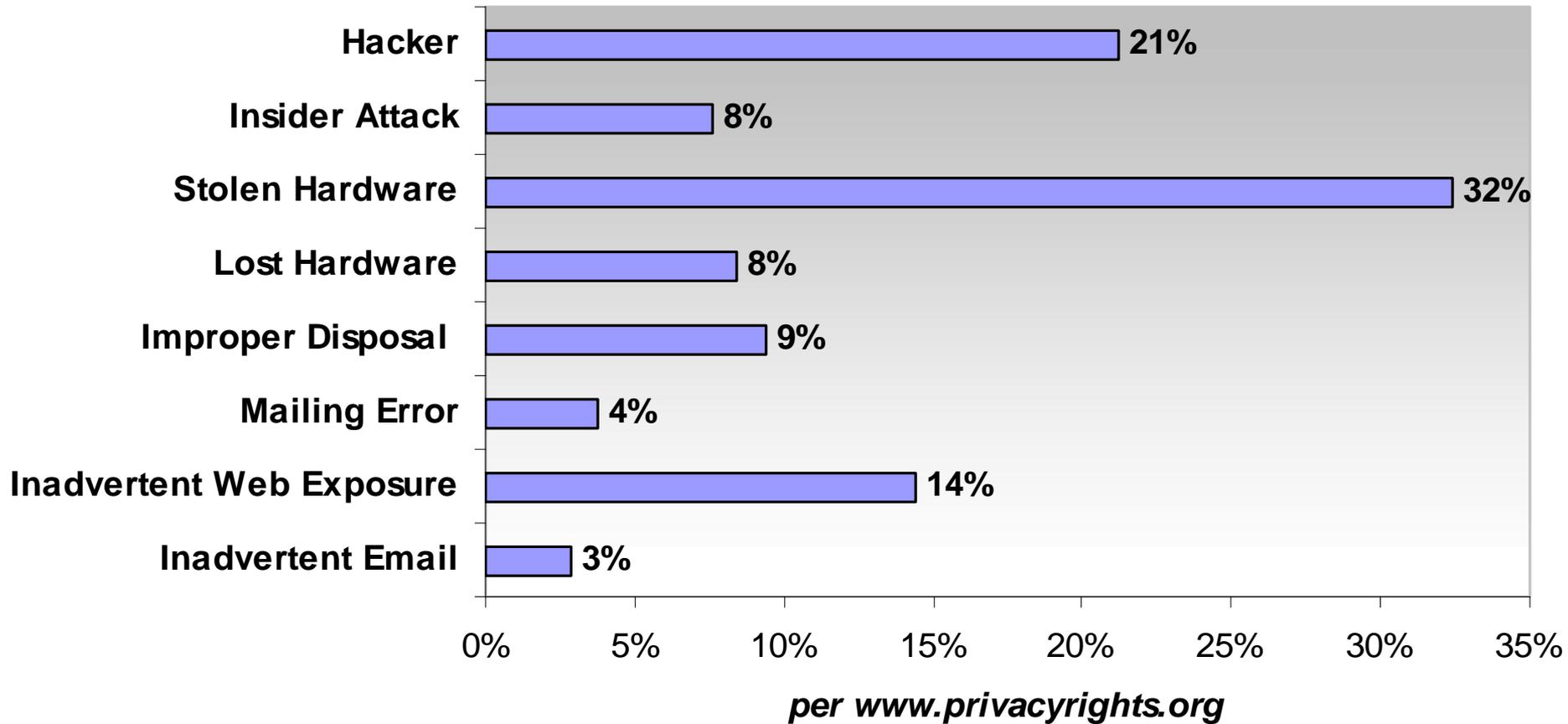
**# of Reported Data Breaches
by Industry 2005-2009**



per www.privacyrights.org

Types of Data Breaches

Reported Data Breaches by Type 2005-2009





Inadvertent EMAIL Leaks

<p>January 2009</p>	<p>Missouri State University</p>	<p>Personal information, including Social Security numbers for 565 foreign students at MSU was leaked when a university office sent an e-mail message soliciting their help with language tutoring. The email message had a spreadsheet attachment that contained names and Social Security numbers for international students.</p>
<p>March 2008</p>	<p>Binghamton University</p>	<p>A university employee mistakenly sent an e-mail attachment containing the names, grade point averages and Social Security numbers accounting students to another group of School of Management students.</p>
<p>Oct 2009</p>	<p>Baptist Hospital East</p>	<p>This Kentucky hospital accidentally released employee social security numbers. 350 names of hospital employees appear on a list that was circulated in an e-mail and so did their Social Security numbers.</p>

Inadvertent EMAIL Leaks

<p>August 2009</p>	<p>National Finance Center</p>	<p>An employee with the National Finance Center mistakenly sent an Excel spreadsheet containing employees' personal information to a co-worker via e-mail in an unencrypted form. The names and Social Security numbers of at least 27,000 Commerce Department employees were exposed.</p>
<p>Sept 2008</p>	<p>Blue Cross Blue Shield</p>	<p>A document containing personal data was accidentally attached to a general e-mail being sent out to brokers notifying them of a software upgrade. Information such as Social Security numbers, phone numbers and addresses were exposed.</p>
<p>June 2008</p>	<p>California Dept of Consumer Affairs</p>	<p>A Microsoft Word document was emailed outside of the department. The document contained the names, salaries, SSN and titles of 5000 people.</p>

Inadvertent EMAIL Leaks

<p>December 2008</p>	<p>New Hampshire Dept. of Health and Human Services</p>	<p>NH Health and Human Services mistakenly released the Social Security numbers and other personal information of Medicare Part D recipients. The information was mistakenly attached to a e-mail to health care organizations including nursing homes.</p>
<p>December 2007</p>	<p>Cameron County</p>	<p>An employee released an e-mail with an attached list of all county officials and employees. It reportedly contained names, Social Security numbers, and salaries.</p>
<p>July 2009</p>	<p>Hampton Redevelopment and Housing Authority</p>	<p>The Social Security numbers and other personal information of nearly 900 people who were banned from public housing in Hampton were accidentally given to a resident who requested the information. A housing authority employee attached a spreadsheet but forgot to exclude the personal information.</p>

Inadvertent EMAIL Leaks

<p>October 2006</p>	<p>Republican National Committee</p>	<p>The Republican National Committee (RNC) inadvertently emailed a list of donors' names, SSNs and races to a New York Sun reporter.</p>
<p>September 2008</p>	<p>Ivy Tech Community College</p>	<p>An employee of the college sent a file that consisted of students enrolled in the spring 2008 semester for distance education courses. The employee intended to send the file to a single employee of the college. Instead, the email was accidentally sent to a list of all Indianapolis region employees.</p>
<p>May 2008</p>	<p>Princeton Tower Club</p>	<p>Tower Club is taking steps to protect 103 of its alumni after a spreadsheet listing their names and Social Security numbers was e-mailed to current club members. The document was attached to an apparently unrelated e-mail that informed current members about a club event.</p>

Inadvertent WEBSITE Leaks

<p>July 2008</p>	<p>Ohio University</p>	<p>A clerical error led to the online posting of the names and Social Security numbers of people who spoke at Ohio University's Centers for Osteopathic Research and Education. A spreadsheet that contained the information was discovered when a nurse found the information last week while conducting online research. In addition to names and Social Security numbers, the spreadsheet included contact numbers, addresses, their speaking topics and federal employer identification numbers.</p>
<p>December 2008</p>	<p>Cal Poly Pomona</p>	<p>A student accessed an Excel file containing his personal information and others while on the Internet. The information includes names, addresses, phone numbers and Social Security numbers.</p>
<p>June 2008</p>	<p>Govt Accounting Office (GAO)</p>	<p>Data from audit reports on Defense Department travel vouchers were inadvertently posted online and included some service members' names, Social Security numbers and addresses.</p>

Inadvertent WEBSITE Leaks

<p>November 2008</p>	<p>Sinclair Community College</p>	<p>The names and Social Security numbers of almost 1,000 employees were inadvertently left open to public view on the Internet for about a year. A spreadsheet with information on people who worked at the school in 2000 and 2001 was placed in a computer folder by an employee. The employee didn't realize the folder could be viewed on the Internet.</p>
<p>November 2007</p>	<p>Montana State University</p>	<p>An Excel spreadsheet with the names and Social Security numbers of 42 people, most of them hired in the summer of 2006, was publicly accessible on MSU's Web site for an undetermined period of time.</p>
<p>March 2005</p>	<p>Kaiser Permanent</p>	<p>Kaiser Permanente included private patient information on systems diagrams posted on the Web.</p>

Inadvertent WEBSITE Leaks

<p>June 2007</p>	<p>American Airlines</p>	<p>Personal information including Social Security numbers of pilots and other employees at American Airlines, including the chief executive, was exposed on a company Web site.</p>
<p>February 2006</p>	<p>Honeywell</p>	<p>Exposed online. Personal information of current and former employees including Social Security numbers and bank account information posted on an Internet Web site.</p>
<p>March 2009</p>	<p>Comcast</p>	<p>A list of over 8,000 Comcast user name and passwords were available to the public via Scribd for two months. Scribd is an online file sharing site. It is believed that a Comcast employee needed to share information with another Comcast employee at another office location and used Scribd as the mechanism to share the file. The employee subsequently forgot to remove the file after it was used.</p>

Inadvertent WEBSITE Leaks

<p>January 2007</p>	<p>Indiana Department of Transportation</p>	<p>The names and SSNs of INDOT employees were inadvertently posted on an internal network computer drive sometime between Sept. 6 and Dec. 4, 2006.</p>
<p>May 2007</p>	<p>Indiana Department of Administration</p>	<p>An employee uploaded a list of certified women and minority business enterprises to the department's Web site and inadvertently included their tax identification numbers, which for some businesses and sole proprietorships is the owner's Social Security number.</p>
<p>June 2007</p>	<p>Lynchburg, Va</p>	<p>Personal information of Lynchburg city employees and retirees was accidentally posted on the city's website. Included in that information were employees' prescription medications.</p>

Inadvertent WEBSITE Leaks

<p>October 2006</p>	<p>Cumberland County, PA</p>	<p>Cumberland County (PA) officials removed salary board meeting minutes from their Web site because they contained the SSNs of 1,200 county employees. The information was included in minutes from meetings.</p>
<p>Feb 2007</p>	<p>Clarksville-Montgomery County middle and high schools</p>	<p>Staff and faculty Social Security numbers were used as the file names of JPEG photos that were taken for yearbook pictures and placed on school system's Web site.</p>
<p>Feb 2007</p>	<p>Connecticut Office of the Comptroller</p>	<p>Personal information of state employees including names and Social Security numbers was inadvertently posted on the Internet in a spreadsheet of vendors used by the state.</p>

Inadvertent WEBSITE Leaks

- **QUESTION:**

Not that its wrong, but do any Virginia agencies have WORD or EXCEL documents posted on their websites?

- **ANSWER:**

Oh yes



site:*.virginia.gov filetype:doc

Search

Advanced Search

Web Show options...

Results 1 - 10 of about 15,100 from *.virginia.gov for filetype:doc.

State Application 7.0 Format

File Format: Microsoft Word - View as HTML

DHRM Form 10-012 (Rev. 9/03). Please print in ink (preferably black) or use typewriter. Number of attachments. Position number. Commonwealth of Virginia ...

jobs.virginia.gov/state6.doc - Similar

by AEO Employer - Related articles - All 4771 versions

Request For Information

File Format: Microsoft Word - View as HTML

Request For Information. "RFI". Date: August 12, 2008. Title: VA STAR: Virginia Student Training and Refurbishment Program. Issuing/Using Entity: Department ...

www.technology.virginia.gov/VA_STAR_Prog_RFI_Final081208.doc - Similar

INFORMATION NETWORK SERVICES AGREEMENT

File Format: Microsoft Word - View as HTML

VIRGINIA INFORMATION PROVIDERS NETWORK. INFORMATION NETWORK SERVICES AGREEMENT. BETWEEN. THE VIRGINIA INFORMATION PROVIDERS NETWORK ...

www.virginia.gov/minutes/DHP.doc - Similar

by A ATTACHMENT - Cited by 1 - Related articles - All 488 versions

INFORMATION NETWORK SERVICES AGREEMENT

File Format: Microsoft Word - View as HTML

INFORMATION NETWORK SERVICES AGREEMENT. between the VIRGINIA INFORMATION PROVIDERS NETWORK. and the VIRGINIA TOURISM CORPORATION. -- DRAFT -- ...

www.virginia.gov/minutes/Phaselenhancementsagreement05_08_01.doc

DRAFT

File Format: Microsoft Word - View as HTML

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT The Virginia Criminal Sentencing Commission

Google Search [Advanced Search](#)

[+ Show options...](#) Results 1 - 10 of about 21,300 from *.state.va.us for filetype:doc. (0.14 seconds)

[Report](#)
Format: Microsoft Word - [View as HTML](#)
John F. Childress, Ph.D. RACSB. P.O. Box 277. Spotsylvania, VA 22553. (540) 582
childress@racsb.state.va.us. Internship Program ...
[sb.state.va.us/2006internpacket.doc](#) - [Similar](#)

[State Application 7.0 Format](#)
Format: Microsoft Word - [View as HTML](#)
Form 10-012 (Rev. 9/03). Please print in ink (preferably black) or use typewriter.
of attachments. Position number. Commonwealth of Virginia ...
[e.va.us/state6.doc](#) - [Similar](#)
Employer - [Related articles](#) - [All 4771 versions](#)

[January 24, 1997](#)
Format: Microsoft Word - [View as HTML](#)
HANNOCK REGIONAL JAIL AUTHORITY. \$39790000 Series 1998 Regional Jail
Revenue Bonds. \$32190000 Series 2006A Regional Jail Facility Revenue ...
[state.va.us/rfjsuccessortrustee.doc](#) - [Similar](#)

[State Application for DCJS P-14](#)
Format: Microsoft Word - [View as HTML](#)
HANNOCK REGIONAL JAIL. An Equal Opportunity Employer. Application for
ment. Type or print all required information. Send completed application to ...
[state.va.us/jailjobapp.doc](#) - [Similar](#)

[Commonwealth of Virginia](#)
Format: Microsoft Word - [View as HTML](#)
al Choice. Certificate of Group Health Plan Coverage. Date of This Certificate: Name of
ant: Name of Health Care Plan: ...
[lncalchoice.state.va.us/HIPAA.Certification.doc](#) - [Similar](#)

Google Search [Advanced Search](#)

Show options... Results 1 - 10 of about 2,290 from *.virginia.gov for filetype:xls. (0.05 second)

[Nutrition Standards Assessment Tool - Virginia Department of Education](#)
Format: Microsoft Excel - [View as HTML](#)
D, E, F, G, H, I, J, K, L, M, N. 1, Product, Servings per container, Weight in grams, Meets standard. CALORIES, Sugar grams, % Sugar by ...
[virginia.gov/nutrition_standards_assessment_tool.xls](#) - [Similar](#)

[Taxable Salary Spreadsheet \(XCEL\) \(download and use on ...](#)
Format: Microsoft Excel - [View as HTML](#)
5, Enter Here, Enter Here, Enter Here, Enter Here, Enter Here, Formula, Formula. 6, Position #, Employee Name, Comp Bd Monthly Salary ...
[virginia.gov/Taxable_Salary.xls](#) - [Similar](#)

[Quarter-Minute Account Order Form - VITA: Home](#)
Format: Microsoft Excel - [View as HTML](#)
D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y, Z. 1. 2. 3, VITA Audio Conferencing Account Order Form. 4, First Name ...
[virginia.gov/accountorder.xls](#) - [Similar](#)

[New Jobs Application Form - Virginia Department of Business Assistance](#)
Format: Microsoft Excel - [View as HTML](#)
D, E, F, G, H, I, J, K, L, M. 1, VIRGINIA JOBS INVESTMENT PROGRAM. 2, NEW APPLICATION. 3. 4, Section I. Company Information ...
[virginia.gov/documents/NewJobsApp2010.XLS](#)

[Top 100 Brands Fiscal Year 2006 - Virginia Department of Alcoholic ...](#)
Format: Microsoft Excel - [View as HTML](#)
D, E, F, G, H, I, J, K, M, N, P, Q, S. 1. 2. 3. 4, Top 100 Brands - Total Dollars / Bottles-Sold. 5, Fiscal Year 2006 v Fiscal Year 2005 ...
[virginia.gov/salesreports/top100Brands.xls](#) - [Similar](#)

Google Search [Advanced Search](#)

Show options... Results 1 - 10 of about 779 from *.state.va.us for filetype:xls. (0.14 seconds)

[Taxable Salary Spreadsheet \(XCEL\) \(download and use on ...](#)
Format: Microsoft Excel - [View as HTML](#)
1, 2, 3, 4, 5, Enter Here, Enter Here, Enter Here, Enter Here, Enter Here, Formula, Formula. 6,
7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30,
31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53,
54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75,
76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97,
98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115,
116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132,
133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 147, 148, 149,
150, 151, 152, 153, 154, 155, 156, 157, 158, 159, 160, 161, 162, 163, 164, 165, 166,
167, 168, 169, 170, 171, 172, 173, 174, 175, 176, 177, 178, 179, 180, 181, 182, 183,
184, 185, 186, 187, 188, 189, 190, 191, 192, 193, 194, 195, 196, 197, 198, 199, 200,
201, 202, 203, 204, 205, 206, 207, 208, 209, 210, 211, 212, 213, 214, 215, 216, 217,
218, 219, 220, 221, 222, 223, 224, 225, 226, 227, 228, 229, 230, 231, 232, 233, 234,
235, 236, 237, 238, 239, 240, 241, 242, 243, 244, 245, 246, 247, 248, 249, 250,
251, 252, 253, 254, 255, 256, 257, 258, 259, 260, 261, 262, 263, 264, 265, 266, 267,
268, 269, 270, 271, 272, 273, 274, 275, 276, 277, 278, 279, 280, 281, 282, 283, 284,
285, 286, 287, 288, 289, 290, 291, 292, 293, 294, 295, 296, 297, 298, 299, 300,
301, 302, 303, 304, 305, 306, 307, 308, 309, 310, 311, 312, 313, 314, 315, 316, 317,
318, 319, 320, 321, 322, 323, 324, 325, 326, 327, 328, 329, 330, 331, 332, 333, 334,
335, 336, 337, 338, 339, 340, 341, 342, 343, 344, 345, 346, 347, 348, 349, 350,
351, 352, 353, 354, 355, 356, 357, 358, 359, 360, 361, 362, 363, 364, 365, 366, 367,
368, 369, 370, 371, 372, 373, 374, 375, 376, 377, 378, 379, 380, 381, 382, 383, 384,
385, 386, 387, 388, 389, 390, 391, 392, 393, 394, 395, 396, 397, 398, 399, 400,
401, 402, 403, 404, 405, 406, 407, 408, 409, 410, 411, 412, 413, 414, 415, 416, 417,
418, 419, 420, 421, 422, 423, 424, 425, 426, 427, 428, 429, 430, 431, 432, 433, 434,
435, 436, 437, 438, 439, 440, 441, 442, 443, 444, 445, 446, 447, 448, 449, 450,
451, 452, 453, 454, 455, 456, 457, 458, 459, 460, 461, 462, 463, 464, 465, 466, 467,
468, 469, 470, 471, 472, 473, 474, 475, 476, 477, 478, 479, 480, 481, 482, 483, 484,
485, 486, 487, 488, 489, 490, 491, 492, 493, 494, 495, 496, 497, 498, 499, 500,
501, 502, 503, 504, 505, 506, 507, 508, 509, 510, 511, 512, 513, 514, 515, 516, 517,
518, 519, 520, 521, 522, 523, 524, 525, 526, 527, 528, 529, 530, 531, 532, 533, 534,
535, 536, 537, 538, 539, 540, 541, 542, 543, 544, 545, 546, 547, 548, 549, 550,
551, 552, 553, 554, 555, 556, 557, 558, 559, 560, 561, 562, 563, 564, 565, 566, 567,
568, 569, 570, 571, 572, 573, 574, 575, 576, 577, 578, 579, 580, 581, 582, 583, 584,
585, 586, 587, 588, 589, 590, 591, 592, 593, 594, 595, 596, 597, 598, 599, 600,
601, 602, 603, 604, 605, 606, 607, 608, 609, 610, 611, 612, 613, 614, 615, 616, 617,
618, 619, 620, 621, 622, 623, 624, 625, 626, 627, 628, 629, 630, 631, 632, 633, 634,
635, 636, 637, 638, 639, 640, 641, 642, 643, 644, 645, 646, 647, 648, 649, 650,
651, 652, 653, 654, 655, 656, 657, 658, 659, 660, 661, 662, 663, 664, 665, 666, 667,
668, 669, 670, 671, 672, 673, 674, 675, 676, 677, 678, 679, 680, 681, 682, 683, 684,
685, 686, 687, 688, 689, 690, 691, 692, 693, 694, 695, 696, 697, 698, 699, 700,
701, 702, 703, 704, 705, 706, 707, 708, 709, 710, 711, 712, 713, 714, 715, 716, 717,
718, 719, 720, 721, 722, 723, 724, 725, 726, 727, 728, 729, 730, 731, 732, 733, 734,
735, 736, 737, 738, 739, 740, 741, 742, 743, 744, 745, 746, 747, 748, 749, 750,
751, 752, 753, 754, 755, 756, 757, 758, 759, 760, 761, 762, 763, 764, 765, 766, 767,
768, 769, 770, 771, 772, 773, 774, 775, 776, 777, 778, 779, 780, 781, 782, 783, 784,
785, 786, 787, 788, 789, 790, 791, 792, 793, 794, 795, 796, 797, 798, 799, 800,
801, 802, 803, 804, 805, 806, 807, 808, 809, 810, 811, 812, 813, 814, 815, 816, 817,
818, 819, 820, 821, 822, 823, 824, 825, 826, 827, 828, 829, 830, 831, 832, 833, 834,
835, 836, 837, 838, 839, 840, 841, 842, 843, 844, 845, 846, 847, 848, 849, 850,
851, 852, 853, 854, 855, 856, 857, 858, 859, 860, 861, 862, 863, 864, 865, 866, 867,
868, 869, 870, 871, 872, 873, 874, 875, 876, 877, 878, 879, 880, 881, 882, 883, 884,
885, 886, 887, 888, 889, 890, 891, 892, 893, 894, 895, 896, 897, 898, 899, 900,
901, 902, 903, 904, 905, 906, 907, 908, 909, 910, 911, 912, 913, 914, 915, 916, 917,
918, 919, 920, 921, 922, 923, 924, 925, 926, 927, 928, 929, 930, 931, 932, 933, 934,
935, 936, 937, 938, 939, 940, 941, 942, 943, 944, 945, 946, 947, 948, 949, 950,
951, 952, 953, 954, 955, 956, 957, 958, 959, 960, 961, 962, 963, 964, 965, 966, 967,
968, 969, 970, 971, 972, 973, 974, 975, 976, 977, 978, 979, 980, 981, 982, 983, 984,
985, 986, 987, 988, 989, 990, 991, 992, 993, 994, 995, 996, 997, 998, 999, 1000,
1001, 1002, 1003, 1004, 1005, 1006, 1007, 1008, 1009, 1010, 1011, 1012, 1013, 1014,
1015, 1016, 1017, 1018, 1019, 1020, 1021, 1022, 1023, 1024, 1025, 1026, 1027, 1028,
1029, 1030, 1031, 1032, 1033, 1034, 1035, 1036, 1037, 1038, 1039, 1040, 1041, 1042,
1043, 1044, 1045, 1046, 1047, 1048, 1049, 1050, 1051, 1052, 1053, 1054, 1055, 1056,
1057, 1058, 1059, 1060, 1061, 1062, 1063, 1064, 1065, 1066, 1067, 1068, 1069, 1070,
1071, 1072, 1073, 1074, 1075, 1076, 1077, 1078, 1079, 1080, 1081, 1082, 1083, 1084,
1085, 1086, 1087, 1088, 1089, 1090, 1091, 1092, 1093, 1094, 1095, 1096, 1097, 1098,
1099, 1100, 1101, 1102, 1103, 1104, 1105, 1106, 1107, 1108, 1109, 1110, 1111, 1112,
1113, 1114, 1115, 1116, 1117, 1118, 1119, 1120, 1121, 1122, 1123, 1124, 1125, 1126,
1127, 1128, 1129, 1130, 1131, 1132, 1133, 1134, 1135, 1136, 1137, 1138, 1139, 1140,
1141, 1142, 1143, 1144, 1145, 1146, 1147, 1148, 1149, 1150, 1151, 1152, 1153, 1154,
1155, 1156, 1157, 1158, 1159, 1160, 1161, 1162, 1163, 1164, 1165, 1166, 1167, 1168,
1169, 1170, 1171, 1172, 1173, 1174, 1175, 1176, 1177, 1178, 1179, 1180, 1181, 1182,
1183, 1184, 1185, 1186, 1187, 1188, 1189, 1190, 1191, 1192, 1193, 1194, 1195, 1196,
1197, 1198, 1199, 1200, 1201, 1202, 1203, 1204, 1205, 1206, 1207, 1208, 1209, 1210,
1211, 1212, 1213, 1214, 1215, 1216, 1217, 1218, 1219, 1220, 1221, 1222, 1223, 1224,
1225, 1226, 1227, 1228, 1229, 1230, 1231, 1232, 1233, 1234, 1235, 1236, 1237, 1238,
1239, 1240, 1241, 1242, 1243, 1244, 1245, 1246, 1247, 1248, 1249, 1250, 1251, 1252,
1253, 1254, 1255, 1256, 1257, 1258, 1259, 1260, 1261, 1262, 1263, 1264, 1265, 1266,
1267, 1268, 1269, 1270, 1271, 1272, 1273, 1274, 1275, 1276, 1277, 1278, 1279, 1280,
1281, 1282, 1283, 1284, 1285, 1286, 1287, 1288, 1289, 1290, 1291, 1292, 1293, 1294,
1295, 1296, 1297, 1298, 1299, 1300, 1301, 1302, 1303, 1304, 1305, 1306, 1307, 1308,
1309, 1310, 1311, 1312, 1313, 1314, 1315, 1316, 1317, 1318, 1319, 1320, 1321, 1322,
1323, 1324, 1325, 1326, 1327, 1328, 1329, 1330, 1331, 1332, 1333, 1334, 1335, 1336,
1337, 1338, 1339, 1340, 1341, 1342, 1343, 1344, 1345, 1346, 1347, 1348, 1349, 1350,
1351, 1352, 1353, 1354, 1355, 1356, 1357, 1358, 1359, 1360, 1361, 1362, 1363, 1364,
1365, 1366, 1367, 1368, 1369, 1370, 1371, 1372, 1373, 1374, 1375, 1376, 1377, 1378,
1379, 1380, 1381, 1382, 1383, 1384, 1385, 1386, 1387, 1388, 1389, 1390, 1391, 1392,
1393, 1394, 1395, 1396, 1397, 1398, 1399, 1400, 1401, 1402, 1403, 1404, 1405, 1406,
1407, 1408, 1409, 1410, 1411, 1412, 1413, 1414, 1415, 1416, 1417, 1418, 1419, 1420,
1421, 1422, 1423, 1424, 1425, 1426, 1427, 1428, 1429, 1430, 1431, 1432, 1433, 1434,
1435, 1436, 1437, 1438, 1439, 1440, 1441, 1442, 1443, 1444, 1445, 1446, 1447, 1448,
1449, 1450, 1451, 1452, 1453, 1454, 1455, 1456, 1457, 1458, 1459, 1460, 1461, 1462,
1463, 1464, 1465, 1466, 1467, 1468, 1469, 1470, 1471, 1472, 1473, 1474, 1475, 1476,
1477, 1478, 1479, 1480, 1481, 1482, 1483, 1484, 1485, 1486, 1487, 1488, 1489, 1490,
1491, 1492, 1493, 1494, 1495, 1496, 1497, 1498, 1499, 1500, 1501, 1502, 1503, 1504,
1505, 1506, 1507, 1508, 1509, 1510, 1511, 1512, 1513, 1514, 1515, 1516, 1517, 1518,
1519, 1520, 1521, 1522, 1523, 1524, 1525, 1526, 1527, 1528, 1529, 1530, 1531, 1532,
1533, 1534, 1535, 1536, 1537, 1538, 1539, 1540, 1541, 1542, 1543, 1544, 1545, 1546,
1547, 1548, 1549, 1550, 1551, 1552, 1553, 1554, 1555, 1556, 1557, 1558, 1559, 1560,
1561, 1562, 1563, 1564, 1565, 1566, 1567, 1568, 1569, 1570, 1571, 1572, 1573, 1574,
1575, 1576, 1577, 1578, 1579, 1580, 1581, 1582, 1583, 1584, 1585, 1586, 1587, 1588,
1589, 1590, 1591, 1592, 1593, 1594, 1595, 1596, 1597, 1598, 1599, 1600, 1601, 1602,
1603, 1604, 1605, 1606, 1607, 1608, 1609, 1610, 1611, 1612, 1613, 1614, 1615, 1616,
1617, 1618, 1619, 1620, 1621, 1622, 1623, 1624, 1625, 1626, 1627, 1628, 1629, 1630,
1631, 1632, 1633, 1634, 1635, 1636, 1637, 1638, 1639, 1640, 1641, 1642, 1643, 1644,
1645, 1646, 1647, 1648, 1649, 1650, 1651, 1652, 1653, 1654, 1655, 1656, 1657, 1658,
1659, 1660, 1661, 1662, 1663, 1664, 1665, 1666, 1667, 1668, 1669, 1670, 1671, 1672,
1673, 1674, 1675, 1676, 1677, 1678, 1679, 1680, 1681, 1682, 1683, 1684, 1685, 1686,
1687, 1688, 1689, 1690, 1691, 1692, 1693, 1694, 1695, 1696, 1697, 1698, 1699, 1700,
1701, 1702, 1703, 1704, 1705, 1706, 1707, 1708, 1709, 1710, 1711, 1712, 1713, 1714,
1715, 1716, 1717, 1718, 1719, 1720, 1721, 1722, 1723, 1724, 1725, 1726, 1727, 1728,
1729, 1730, 1731, 1732, 1733, 1734, 1735, 1736, 1737, 1738, 1739, 1740, 1741, 1742,
1743, 1744, 1745, 1746, 1747, 1748, 1749, 1750, 1751, 1752, 1753, 1754, 1755, 1756,
1757, 1758, 1759, 1760, 1761, 1762, 1763, 1764, 1765, 1766, 1767, 1768, 1769, 1770,
1771, 1772, 1773, 1774, 1775, 1776, 1777, 1778, 1779, 1780, 1781, 1782, 1783, 1784,
1785, 1786, 1787, 1788, 1789, 1790, 1791, 1792, 1793, 1794, 1795, 1796, 1797, 1798,
1799, 1800, 1801, 1802, 1803, 1804, 1805, 1806, 1807, 1808, 1809, 1810, 1811, 1812,
1813, 1814, 1815, 1816, 1817, 1818, 1819, 1820, 1821, 1822, 1823, 1824, 1825, 1826,
1827, 1828, 1829, 1830, 1831, 1832, 1833, 1834, 1835, 1836, 1837, 1838, 1839, 1840,
1841, 1842, 1843, 1844, 1845, 1846, 1847, 1848, 1849, 1850, 1851, 1852, 1853, 1854,
1855, 1856, 1857, 1858, 1859, 1860, 1861, 1862, 1863, 1864, 1865, 1866, 1867, 1868,
1869, 1870, 1871, 1872, 1873, 1874, 1875, 1876, 1877, 1878, 1879, 1880, 1881, 1882,
1883, 1884, 1885, 1886, 1887, 1888, 1889, 1890, 1891, 1892, 1893, 1894, 1895, 1896,
1897, 1898, 1899, 1900, 1901, 1902, 1903, 1904, 1905, 1906, 1907, 1908, 1909, 1910,
1911, 1912, 1913, 1914, 1915, 1916, 1917, 1918, 1919, 1920, 1921, 1922, 1923, 1924,
1925, 1926, 1927, 1928, 1929, 1930, 1931, 1932, 1933, 1934, 1935, 1936, 1937, 1938,
1939, 1940, 1941, 1942, 1943, 1944, 1945, 1946, 1947, 1948, 1949, 1950, 1951, 1952,
1953, 1954, 1955, 1956, 1957, 1958, 1959, 1960, 1961, 1962, 1963, 1964, 1965, 1966,
1967, 1968, 1969, 1970, 1971, 1972, 1973, 1974, 1975, 1976, 1977, 1978, 1979, 1980,
1981, 1982, 1983, 1984, 1985, 1986, 1987, 1988, 1989, 1990, 1991, 1992, 1993, 1994,
1995, 1996, 1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008,
2009, 2010, 2011, 2012, 2013, 2014, 2015, 2016, 2017, 2018, 2019, 2020, 2021, 2022,
2023, 2024, 2025, 2026, 2027, 2028, 2029, 2030, 2031, 2032, 2033, 2034, 2035, 2036,
2037, 2038, 2039, 2040, 2041, 2042, 2043, 2044, 2045, 2046, 2047, 2048, 2049, 2050,
2051, 2052, 2053, 2054, 2055, 2056, 2057, 2058, 2059, 2060, 2061, 2062, 2063, 2064,
2065, 2066, 2067, 2068, 2069, 2070, 2071, 2072, 2073, 2074, 2075, 2076, 2077, 2078,
2079, 2080, 2081, 2082, 2083, 2084, 2085, 2086, 2087, 2088, 2089, 2090, 2091, 2092,
2093, 2094, 2095, 2096, 2097, 2098, 2099, 2100, 2101, 2102, 2103, 2104, 2105, 2106,
2107, 2108, 2109, 2110, 2111, 2112, 2113, 2114, 2115, 2116, 2117, 2118, 2119, 2120,
2121, 2122, 2123, 2124, 2125, 2126, 2127, 2128, 2129, 2130, 2131, 2132, 2133, 2134,
2135, 2136, 2137, 2138, 2139, 2140, 2141, 2142, 2143, 2144, 2145, 2146, 2147, 2148,
2149, 2150, 2151, 2152, 2153, 2154, 2155, 2156, 2157, 2158, 2159, 2160, 2161, 2162,
2163, 2164, 2165, 2166, 2167, 2168, 2169,

Ok, let's review:

15,100 MS Word files on virginia.gov

21,300 MS Word files on state.va.us

2,290 MS Excel files on virginia.gov

779 MS Excel files on state.va.us

That's roughly 40,000 Word and Excel files

That's not counting *.edu, *.org, *.com
domains that belong to State agencies

In August 2009, CESC email servers sent over **6.1 million** outgoing emails. Assuming that August is an average month in terms of volume, that means that over 73 million emails are sent per year just through CESC email servers. If only 5% of those emails had a Word or Excel document attached, that's 3.6 million additional chances to leak data. Even if it's only 1%, that's still 730,000 opportunities. That's not counting emails sent by universities, judicial, legislative and other non-partnership agencies.

The electronic movement of information between our employees and people outside the agency is a fundamental requirement for most agencies. The Web, and the use of e-mail, has simplified the process, but has also opened up numerous vulnerabilities.



At the Commonwealth, these files are never sensitive. Right? Because all Word and Excel files are checked, double-checked and triple-checked before they're posted to a website or emailed or somehow sent to another party to make certain that there is no sensitive data. Right? RIGHT?

In general, my experience tells me that Commonwealth employees are VERY conscientious when it comes to securing sensitive data.

But...my experience also tells me that sometimes Word files and Excel files are not always exactly what they appear to be.

Sometimes...WYSI<NOT>WYG

Just ask this guy



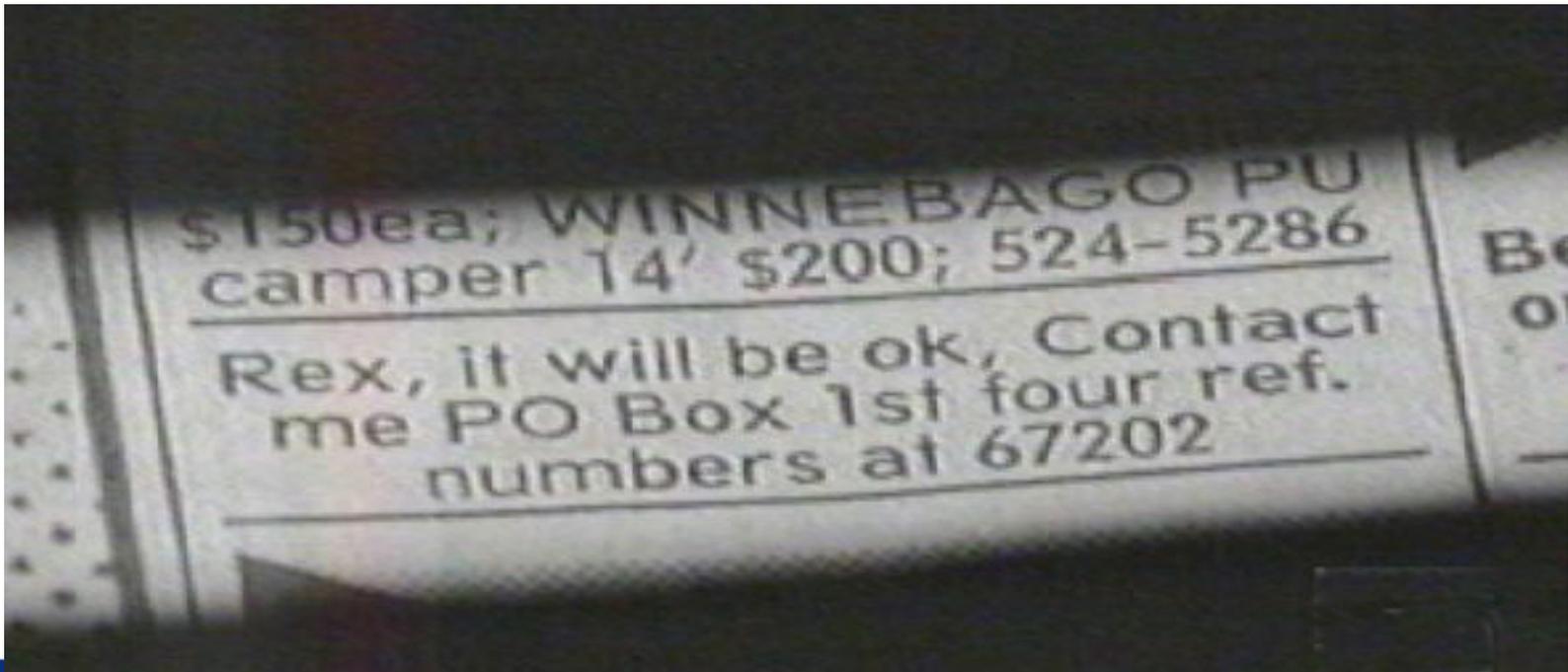
“The floppy did me in.”

The BTK Killer

BTK was a serial killer who murdered at least ten people in the Wichita, Kansas area, over a 30 year period from 1974 to 2004. He gave himself the initials of BTK, which stands for Bind, Torture, and Kill.

BTK wrote many letters to the press and the police after the killing sprees in his early years, boasting of the crimes and knowledge of details. After a long hiatus, these letters resumed in 2004.

In early 2005, using coded messages in newspaper ads, BTK asked the police if they could trace a floppy disk if he gave them one. Using the agreed upon code, the police responded in another ad, assuring BTK that it would be “ok”, they could not trace a floppy disk.



On Feb. 16, 2005 BTK sent a package to Wichita's Fox KAKE television affiliate that contained some index cards and a purple floppy disk. The package was promptly turned over to police.



On the Disk

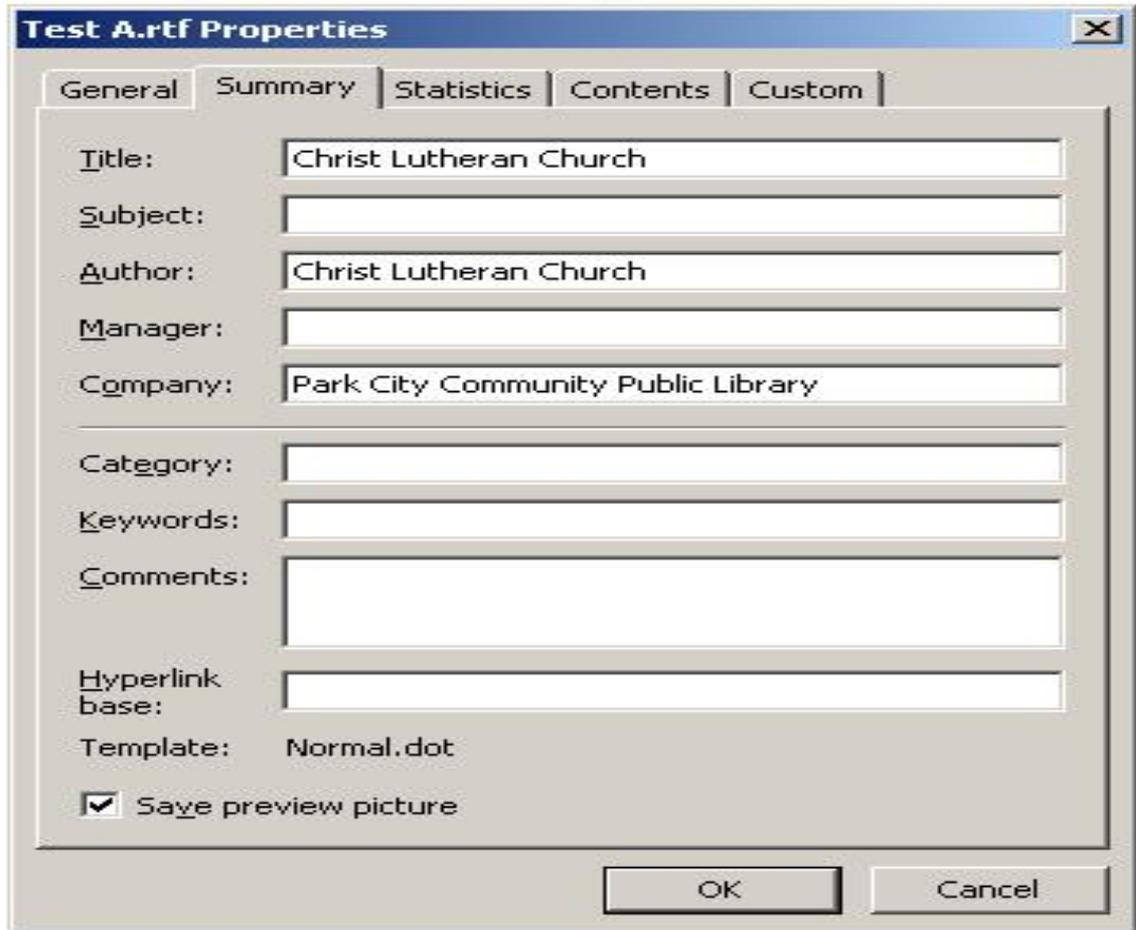
Using the Encase forensic tool, the police examiners recovered a deleted file titled 'Test A.RTF.' from the floppy disk. RTF files are common “rich text format” files that can be used in MS Word as well as many other word processing programs.



File-CLICK

Properties-CLICK

And the police were able to see the author of "Christ Lutheran Church" and a company of "Park City Community Public Library".





This is a test. See 3 X 5 Card for details on communica

Statistics-CLICK

And the police were able to see the file was last saved by "Dennis".

Test A.rtf Properties

General | Summary | **Statistics** | Contents | Custom

Created: Thursday, February 10, 2005 6:05:00 PM
Modified: Monday, February 14, 2005 2:47:44 PM
Accessed: Monday, February 14, 2005
Printed: Monday, February 14, 2005 2:44:00 PM

Last saved by: Dennis
Revision number: 4
Total editing time: 22 Minutes

Statistics:

Statistic name	Value
Pages:	1
Paragraphs:	1
Lines:	1
Words:	18
Characters:	68
Characters (with spaces):	85

OK Cancel



Christ Lutheran Church
Wichita, Kansas

NAVIGATION

[Calendar](#)
[Church](#)
[Classes](#)
[History](#)
[Links](#)
[Map](#)
[Music](#)
[Outreach](#)
[People](#)
[Pictures](#)
[Sermon](#)

Our Congregation council officers look to the future...

President: Dennis Rader

Vice President: Paul Shaw

Secretary: Walter Dietz

Treasurer: Alan Wondra

The Mission of Christ Lutheran Church is to enhance faith

Meaningful and expressive worship;

Pastor: Michael Clark

Worship Chair: Elmer Hoyer

Organists: Freyja Carlstedt and Margaret Dietz

Altar Guild: Deborah Bischoff

Choir Director: Greg Golding

Lifelong learning and growth in faith:

A Google search later and the police were looking at the website of the Christ Lutheran Church in Wichita, Kansas.

CLICK on the "People" and the name of "Dennis Rader" is listed as the President of the Congregation council.





For over 30 years, no names had surfaced as viable leads to the identity of the BTK killer. In just minutes, however, of examining a short simple Word file that was sent on February 16th, Dennis Rader became a person of interest in the case. Within hours of that, he was a prime suspect. He was arrested on February 25th and confessed the following day.

This was excellent police work, but it wasn't rocket science either. The police used advanced forensic tools but they really didn't need them. Dennis Rader got tripped up in the same way that many of those organizations that suffered data breaches were tripped up.

When it comes to Word, Excel, Powerpoint, JPG's, Adobe Acrobat, and many other types of files:

Sometimes:

What-You-See-Is-<NOT>-What-You-Get

Metadata refers to “data about data”. In general, metadata is the data that is associated with a document, but is not generally visible in the ordinary display or printing of the document. Some typical examples include comments, markup and revisions, author, owner and other information, and even records of versions. It can also include forgotten data that may be hidden, obscured or embedded in the document.

~Dennis Kennedy

Show & Tell



Types of Metadata

Track Changes: Inserted or deleted text you thought was gone

Comments

Your name

Your initials

Your email address

Your agency's name

The name of your computer

The name of the network server or hard disk on which you saved the document

Other file properties and summary information

The names of previous document authors

Document revisions

Document versions

Template information

Hidden text

Macros

Hyperlinks

Routing information

Non-visible portions of embedded Object Linking and Embedding (OLE) objects



How do we avoid these problems?

Create a Metadata Policy: Determine what metadata is at risk to your agency and why.

Create guidelines for cleaning: The determination of what and how to clean a document file should be defined by the agency and not by individual users. First of all, it's not wise to depend on users to understand the intricacies and significance of metadata removal. Second, metadata cleanup should be performed consistently throughout the agency and not ad hoc.

How do we avoid these problems?

Start clean: Start from scratch if you can or at least disconnect the document from its past life. Copy & paste the body of the old document into a shell created with new document templates.

Edit clean: Avoid using “Versions”. Instead, create a folder for backups and regularly save numbered copies as a document goes through revisions.



How do we avoid these problems?

Careful with Track Changes: The “Track changes” feature in MS Word is basically a recording device. Word is recording everything that is done to the file. Every user, every hard drive path, every bit of deletion, insertion, copy cut and pasted data is there. In the end, you may have a document that contains all kinds of data you may not realize is there - data you really don't want to share.

How do we avoid these problems?

Familiarize yourself with the application's security features. In MS Word, click Tools|Option and review the security tab.

The screenshot shows the 'Options' dialog box in Microsoft Word, with the 'Security' tab selected. The 'Privacy options' section is circled in red. The 'Security' tab is highlighted with a dotted border. The 'Privacy options' section contains four checked items: 'Remove personal information from file properties on save', 'Warn before printing, saving or sending a file that contains tracked changes or comments', 'Store random number to improve merge accuracy', and 'Make hidden markup visible when opening or saving'. The 'Macro security' section is also visible at the bottom.

Options [?] [X]

User Information Compatibility File Locations
View General Edit Print Save
Security Spelling & Grammar Track Changes

File encryption options for this document _____
Password to open: [] [Advanced...]

File sharing options for this document _____
Password to modify: []

Read-only recommended
[Digital Signatures...] [Protect Document...]

Privacy options

- Remove personal information from file properties on save
- Warn before printing, saving or sending a file that contains tracked changes or comments
- Store random number to improve merge accuracy
- Make hidden markup visible when opening or saving

Macro security

Adjust the security level for opening files that might contain macro viruses and specify the names of trusted macro developers. [Macro Security...]

[OK] [Cancel]



How do we avoid these problems?

Don't send it, publish it. Users must practice appropriate procedures when sending or sharing an electronic copy of a file with outsiders. Publishing a document means following electronic cleanup procedures such as removing comments, undesired Track Changes or other unwanted information.

Use Acrobat PDF files: Encourage the use of PDF files for web sites and email attachments. PDF's have metadata also, but it can be managed and reviewed a little easier.

How do we avoid these problems?

Metadata Application Removal Tools: There are metadata application tools that can help identify and remove metadata.

Content Monitoring Tools: There are also content monitoring tools that scan outgoing email for content or undesired file types.



Thank you.



Enterprise Server Lifecycle Process

Eric Taylor – Enterprise Security Architect
David Matthews – Manager , Server Services

December 2009



NORTHROP GRUMMAN

Agenda

- Server Lifecycle Overview
- Security Requirements
- Security Checklist
 - *Security Compliance Management Toolkit series*
- Partnership Specifics
- References
- Summary

Server Lifecycle Overview

- Standardizing all server builds across an the enterprise
- Ensures security baselines are applied
- Ensures supportability with standard look and feel
- Ensures all enterprise tools are deployed
- System development life cycle

Security Requirements

- Required IAW Sec 501, Section 4.3 IT System Hardening
 - IT System Hardening requirements delineate technical security controls to protect IT systems against security vulnerabilities.
 - Identify, document, and apply appropriate baseline security configurations to all agency IT systems, *regardless of their sensitivity*.
- Systems Development Lifecycle Security
 - Project Initiation – Requirements meetings
 - Implementation – Security scans prior to deployment into production
 - Production - continually monitor systems for security baselines and policy compliance.
 - Disposition - removal of systems from management systems

Security Checklist Template

- Based on the comprehensive checklists produced by CIS, when available
- IT Systems best practices
- Vendor best practices
 - Microsoft Corporation's **Security Compliance Management Toolkit** series
 - Cisco's Guide to Harden Cisco IOS Devices
 - UNIX / Linux best practices

Security Compliance Management Toolkit series

- **Security guide** – The toolkits include updated security guides for Windows Vista, Windows XP, Windows Server 2008, Windows Server 2003, and 2007 Microsoft Office. The guidance provides you with best practices and automated tools to help you plan and deploy your security baselines.
- **Attack Surface Reference workbook** – A resource that lists the changes introduced as server roles are installed on computers running Windows Server 2003 and Windows Server 2008.
- **Security Baseline Settings workbook** – A resource that lists all of the prescribed settings for each of the preconfigured security baselines that the guides recommend.
- **Security Baseline XML** – XML files that allow your organization to consume the data defined in the security baseline settings workbooks.

Security Compliance Management Toolkit series

- **GPOAccelerator tool** – A tool that you can use to create all the Group Policy objects (GPOs) you need to deploy your chosen security configuration. This release also supports Windows Server 2003, and creating security configurations on machines not joined to a domain.
- **INF Files** – INF files for Windows XP, Windows Vista, Windows Server 2003, Windows Server 2008.
- **Baseline Compliance Management Overview** – The overview discusses best practices on how to monitor security baselines for Windows operating systems and Office applications.

Partnership Specifics

What's happening ?

- NG is standardizing all server builds across the Commonwealth – Tracked through the Security IPT.
- Centrally located information - an official repository for instructions and processes for managing servers' lifecycles.
- Transformed network access limitation to the website.
- Server Services Team Members – required to use the material available on the website only.



In the beginning...

- Server Requests – Server Implementation Overview

 - Request for Service (RFS)

 - Customer

 - Internal to NG (non-RFS)

 - ServiceCenter Service Request

- Server Build Information

 - Implementation Process

 - Server Work Order & Instructions

 - Naming Conventions for Windows, UNIX and LINUX Servers

 - Build Instruction

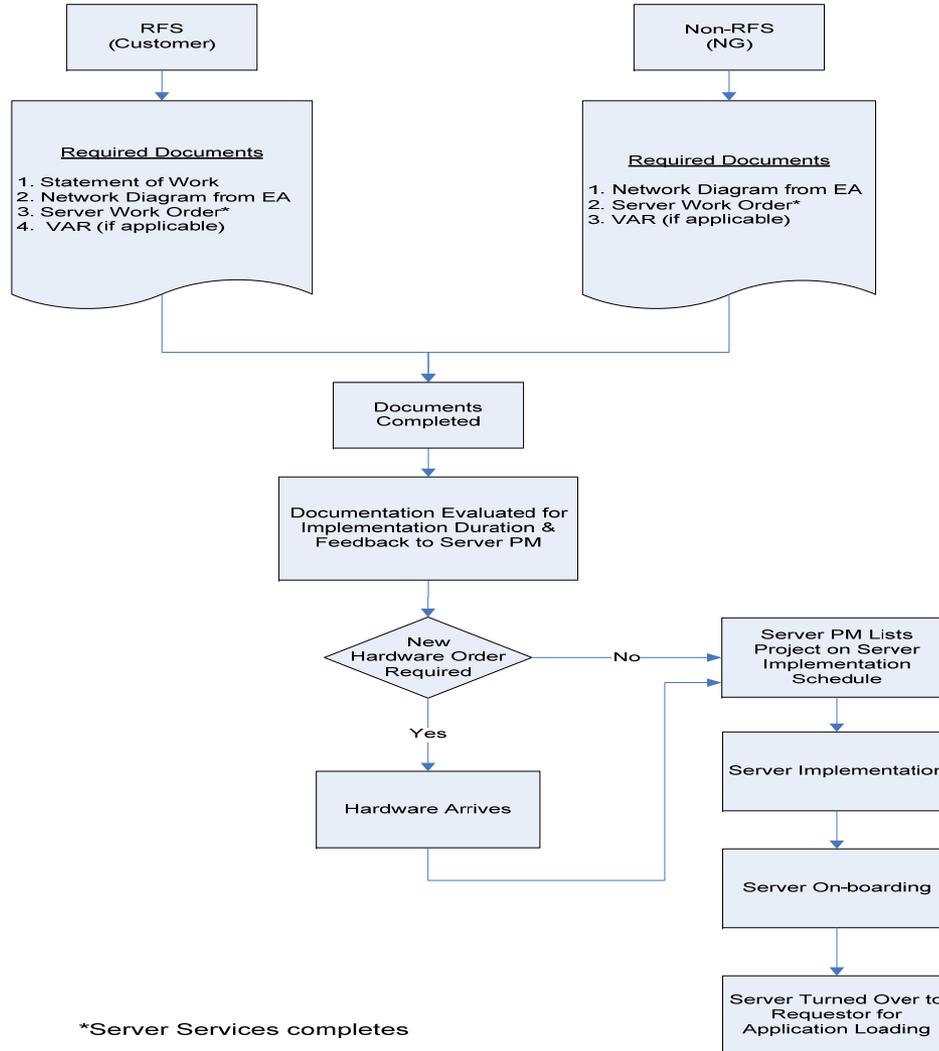
 - Firewall Rules Template

 - PSO Hardening SharePoint Site

 - On-boarding



Server Implementation Request Diagram



Server Work Order

Production and Test Systems

- Designation
- Function / Role
- Hardware
- Operating System
- CPU
- RAM
- Disk
- NICs
- VLANs
- Backup Type
- Special Considerations

Operating System Selections



2000 SP4 Standard and Enterprise



2003 R2 SP2 x86 & x64 Standard and Enterprise



2008 RS x86 & x64 Standard and Enterprise

LINUX



UNIX



Get n-Board!

Create a ServiceCenter Change Request (CR)
Server On-boarding includes:

- ✓ Checklist
- ✓ Technical Training
- ✓ CMDB Template
- ✓ CMDB Instructions - Field Reference
- ✓ Checklist Template

Security Checklist Template

- Requires Server or Service Delivery to fill in checklist
 - Yes and No
 - No requires explanation
- Checklist is sent to Security Operations for verification scans using Security Expressions
 - Prior to turn over to Agency or developers
 - Second scan before production release
- Checklist and Scan results will be archived for future use

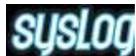
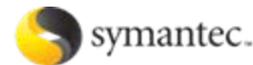
Server Management Tools & Instructions

Installation Procedures & Software



HP-UX **REDHAT** **SUN SOLARIS**

WINDOWS



Server Surplus



Summary

- Standardization of build process
- Established security baseline configurations
- Security compliance with industry best practices and Sec 501
- Automated verification process

References

- *Security Compliance Management Toolkit* series –
 - <http://technet.microsoft.com/en-us/library/cc677002.aspx>
- Cisco's Guide to Harden Cisco IOS Devices –
 - http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080120f48.shtml
- CIS Checklist –
 - www.cisecurity.org/benchmarks.html



Partnership Update

Don Kendrick

Senior Manager, Security Operations Division





Upcoming Events





General Assembly

**General Assembly convenes
January 13, 2010**



Future ISOAG's

From 1:00 – 4:00 pm at CESC

(please let us know if you want to host in the Richmond area!)

Wednesday - January 13, 2010

Wednesday - February 10, 2010

Wednesday - March 10, 2010



Future IS Orientation Sessions

- | | | |
|----------|------------------|--------------------|
| Monday - | January 11, 2010 | 1:00 – 3:30 (CESC) |
| Monday - | February 1, 2010 | 1:00 – 3:30 (CESC) |
| Monday - | March 1, 2010 | 1:00 – 3:30 (CESC) |



MS-ISAC Webcast

National Webcast!

Wednesday, December 16, 2009, 2:00 to 3:00 p.m.

Topic: Phishing Scams – Don't Get Hooked (Part II)

The National Webcast Initiative is a collaborative effort between government and the private sector to help strengthen our Nation's cyber readiness and resilience. A number of vendors have offered their services at no cost, to help develop and deliver the webcasts.

Register @: <http://www.msisac.org/webcast/>



Information Security System Association

ISSA meets on the second Wednesday of every month

DATE: Wednesday, January 13, 2010

LOCATION: Maggiano's Little Italy, 11800 W. Broad St.,
#2204, Richmond/Short Pump Mall

TIME: 11:30 - 1:30pm. Presentation starts at 11:45 &
Lunch served at 12.

PRESENTATION: TBD

COST: ISSA Members: \$15 & Non-Members: \$25



Identity Theft Red Flags Rules Extended Until June 1, 2010

The Red Flags Rule requires many businesses and organizations to implement a written Identify Theft Prevention Program designed to detect the warning signs – or “red flags” – of identity theft in their day-to-day operations.

At the request of members of Congress, the Federal Trade Commission is delaying enforcement of the “Red Flags” Rule until June 1, 2010. Read the FAQ at:

<http://www.ftc.gov/bcp/edu/microsites/redflagesrule/index.shtml>



Security Awareness Tools

Happy Holidays!

For those of you here in Chester we have Security Awareness Tools available for you!

2010 Security Calendars !

Security Bookmarks!

Duh's of Security DVD!

- Distribution at tables in back of conference room
- 1 DVD per entity & signature required



Any Other Business ???????





ADJOURN

THANK YOU FOR ATTENDING AND
MAY YOU AND YOURS ENJOY....

