Virginia Information Technologies Agency

Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

September 9, 2009

September

Virginia Information Technologies Agency

ISOAG September 2009 Agenda

I.	Welcome & Opening Remarks	John Green, VITA
II.	Critical Infrastructure Protection	Mike McAllister, Office of Commonwealth Preparedness
III.	Identity Theft Prevention Program Implementation	Steve Werby, VCU
IV.	COV Security Council Encryption Committee	Steve Werby, VCU
V.	Initial Risk Assessment Process	Eric Taylor, NG
VI.	COV Security Standard 2009 Revisions	John Green, VITA
VII.	2009 Commonwealth Security Data Points	Benny Ambler, VITA
VIII.	Exceptional Exception Processing	Bob Baskette, VITA
IX.	Keys to the Kingdom: Encryption Mechanics & Key Mgmt	Bob Baskette, VITA
X.	Upcoming Events and Other Business	John Green, VITA

Governor's Office of Commonwealth Preparedness

Critical Infrastructure Protection

Mike McAllister

Critical Infrastructure Coordinator

http://www.ocp.virginia.gov/Initiatives/CIP.cfm

VCIPRSP

- Virginia Critical Infrastructure Protection and Resiliency Strategic Plan – Counterpart to the DHS National Infrastructure Protection Plan (NIPP)
- These documents provide unifying structure for integration of existing and future Critical Infrastructure and Key Resources (CIKR) protection efforts and resiliency strategies

http://www.ocp.virginia.gov/Initiatives/CIP.cfm

VCIPRSP

- Objectives include:
  - Understanding and sharing information about terrorist threats and other hazards with CIKR partners
  - Building partnerships to share information and implement CIKR protection programs
  - Implementing a long-term risk management program
  - Maximizing the efficient use of resources for CIKR protection, restoration, and recovery

http://www.ocp.virginia.gov/Initiatives/CIP.cfm

VCIPRSP

- Sector Specific Plan (SSP) Development Current Status:
  - All 18 SSP's under review by OCP
  - Conduct/Continue outreach to private sector to gain input to SSP and establish partnerships

http://www.ocp.virginia.gov/Initiatives/CIP.cfm

Local Outreach

- Concurrent with SSA activity
- Local program to initially deploy to Hampton Roads
- A framework to enhance sector partnership
- Model will promote and facilitate sector and cross-sector planning, collaboration and information sharing for CIKR protection involving all levels of government and private sector entities

http://www.ocp.virginia.gov/Initiatives/CIP.cfm

DHS C/ACAMS

- An aid to information sharing
- Constellation/Automated Critical Asset Management System (C/ACAMS)
  - Collect, store, and share classified and unclassified CIKR data
  - Collect data via secure means, either remotely at CIKR sites or locally at fusion centers
  - Allow limited access to private sector entities, in accordance with established legal frameworks (such as the Protected Critical Infrastructure Information (PCII) program), to facilitate data collection directly from CIKR owners and operators

http://www.ocp.virginia.gov/Initiatives/CIP.cfm

DHS C/ACAMS continued

- Access a comprehensive set of tools and resources to develop and implement critical infrastructure programs
- Allow the user to manage the collection and effective use of CIKR-related data
- Focus on pre-incident prevention and protection, but also assist in post-incident response and recovery operations

http://www.ocp.virginia.gov/Initiatives/CIP.cfm

DHS C/ACAMS Continued

- Current partners:
  - VSP (System Administrator),
  - Fairfax County Police Department (Northern Virginia Coordinator),
  - Virginia Capitol Police,
  - VDOT,
  - Local government emergency managers

http://www.ocp.virginia.gov/Initiatives/CIP.cfm

DHS C/ACAMS Continued

- DHS training requirement: 4 ½ days (no cost)
- Future classes to be conducted in Hampton Roads, Northern Virginia, Southwest Virginia, and Richmond
- Supports identification of CIKR assets for DHS Tier 1 and Tier 2 Program

http://www.ocp.virginia.gov/Initiatives/CIP.cfm

CIKR Asset Identification

- Annual DHS Requirement (National Critical Infrastructure Prioritization Program)
- Introduced a “New” Tier 1/Tier 2 Program
- Moved from “capacity” to “consequence” based criteria
- Enhances ability to capture “criticality” not possible to capture using capacity-based criteria

http://www.ocp.virginia.gov/Initiatives/CIP.cfm

CIKR (Continued)

Tier 2 Criteria: (EXAMPLE)

- 1. Greater than 2500 prompt fatalities;
- 2. Greater than $25 billion in first year economic consequence;
- 3. Mass evacuation with a prolonged absence of greater than 1 month;
- 4. Severe degradation of the country's national security capabilities to include intelligence and defense function, but excluding military facilities

http://www.ocp.virginia.gov/Initiatives/CIP.cfm

CIKR (Continued)

Impact

- Potential to reduce number of assets identified as Tier 1 and Tier 2
- Process now requires analysis of “cluster” assets to achieve consequence based criteria
- Expanded lists derived from “cluster” analysis focus ensures infrastructure does not “fall off” the radar

http://www.ocp.virginia.gov/Initiatives/CIP.cfm

Cyber Security

- First Responder Authentication Credential (FRAC)
- Virginia first in the nation to issue FRAC

http://www.ocp.virginia.gov/Initiatives/CIP.cfm

Virginia FRAC

- 2,300 FRACs issued in Northern Virginia
- Up to 2,000 additional FRACs will be issued in Northern Virginia commencing in October 2009
- FRAC issuance in Hampton Roads commences October 2009
- Approximately 5,700 FRACs will be issued
- Continue expansion to other jurisdictions
- Grant funding secured to support issuance of up to 8,000 additional FRACs
- Public and Private participation
- Institutionalize as a business process

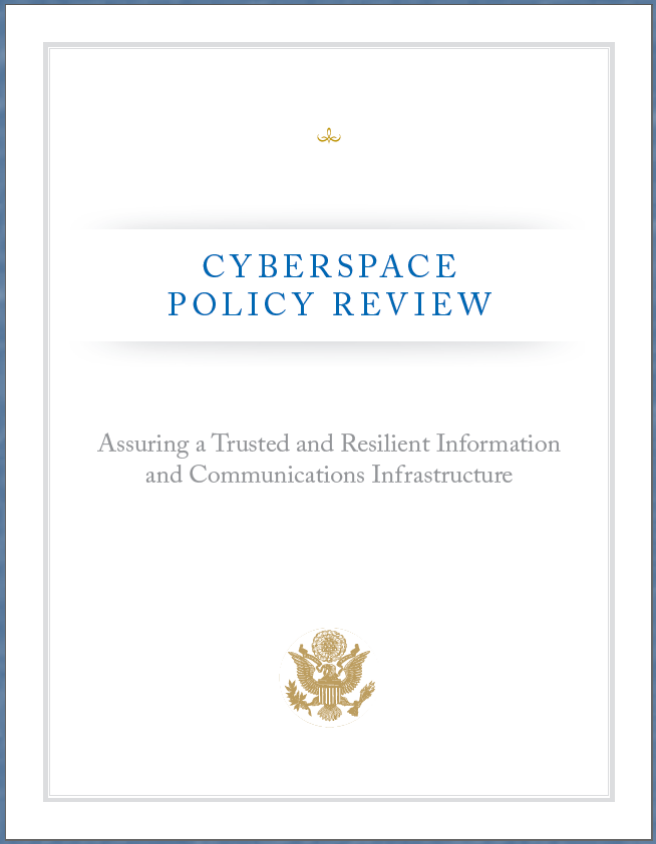
http://www.ocp.virginia.gov/Initiatives/CIP.cfm

Cyber Security

Cyber Security Supports Virginia FRAC Concept

"The President directed a 60-day, comprehensive, "clean-slate" review to assess U.S. policies and structures for cybersecurity."

Policy review issued May 29, 2009.


CYBERSPACE
POLICY REVIEW

Assuring a Trusted and Resilient Information and Communications Infrastructure

http://www.ocp.virginia.gov/Initiatives/CIP.cfm

Cyber Security

Excerpt from “Cyberspace Policy Review”:

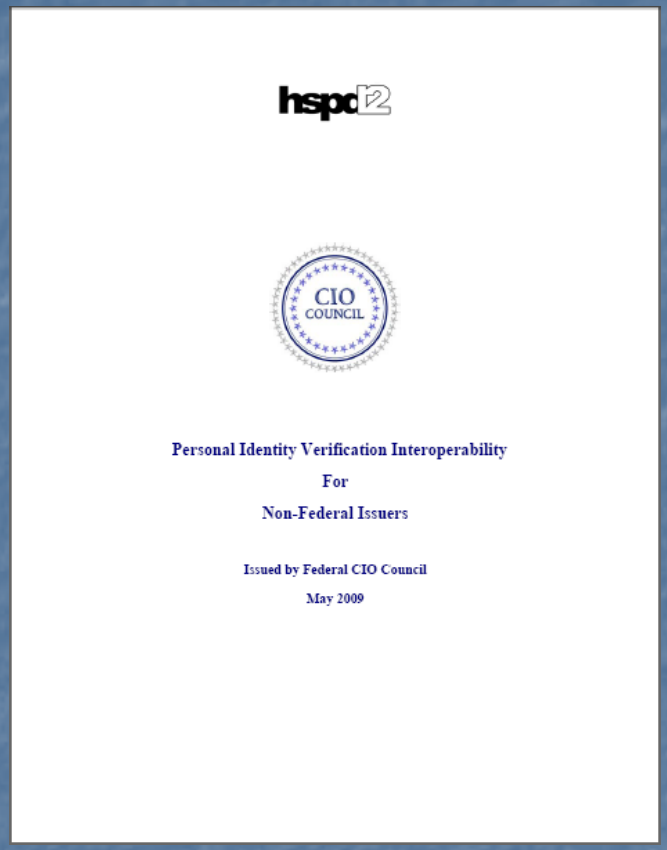
“The Federal government, following the guidance of Homeland Security Presidential Directive 12 (HSPD-12), is seeking to leverage the federal interoperable identity credentialing mechanism across the federal enterprise.”

“The Federal government also should consider extending the availability of federal identity management systems to operators of critical infrastructure and to private-sector emergency response and repair service providers for use during national emergencies.”

http://www.ocp.virginia.gov/Initiatives/CIP.cfm

Federal CIO Council

Virginia FRAC Recognized as Interoperable with Federal Credentials



hspd12

CIO COUNCIL

Personal Identity Verification Interoperability

For

Non-Federal Issuers

Issued by Federal CIO Council

May 2009

http://www.ocp.virginia.gov/Initiatives/CIP.cfm

Federal CIO Council

Excerpt from "Personal Identity Verification (PIV) for Non-Federal Issuers":

"[Enables]...non-federal organizations ... to issue identity cards that are (a) technically interoperable with Federal government PIV systems, and (b) issued in a manner that allows Federal government relying parties to trust the cards. Furthermore, such interoperability and trust may be driven by operational imperatives of great interest to the Federal government (e.g. First Responder Authentication Card (FRAC))."

http://www.ocp.virginia.gov/Initiatives/CIP.cfm

SCP CIP Sub Panel

- The Critical Infrastructure Sub Panel focuses mainly on the implementation of the Virginia Critical Infrastructure Protection and Resiliency Strategic Plan (VCIPRSP), Sector Specific Plans (SSPs), Homeland Security Information Network—Critical Sectors/ Virginia Information Sharing Working Group (VISWG), and DHS Data Calls. The Sub Panel engages with each Sector Specific Agency (SSA) to define SSP planning capabilities and status, and importantly, outreach into the private sector.

http://www.ocp.virginia.gov/Initiatives/CIP.cfm

BZPP

- The Buffer Zone Protection Program (BZPP) supports the implementation of preventive and protective measures outside the perimeter of selected critical infrastructure and key resource (CI/KR) sites throughout the United States. Buffer Zone Plans (BZPs) define supplemental security areas outside the CI/KR site perimeter and recommend preventive and protective measures designed to make it more difficult for terrorists to conduct surveillance or launch attacks. The BZPP provides funding to responsible jurisdictions to purchase equipment to extend the zone of protection around CI/KR facilities, expand preparedness capabilities, and enhance the security of surrounding communities. There were four (4) sites approved in 2007 that received grant money. There is one (1) site approved for 2008.

http://www.ocp.virginia.gov/Initiatives/CIP.cfm

PCII

- The Protected Critical Infrastructure Information (PCII) Program is an information-protection program that enhances information sharing between the private sector and the government. The Department of Homeland Security and other federal, state and local analysts use PCII to analyze and secure critical infrastructure and protected systems, identify vulnerabilities and develop risk assessments, and to enhance recovery preparedness measures.
- If the information submitted satisfies the requirements of the Critical Infrastructure Information Act of 2002*)*, it is protected from:

  The Freedom of Information Act (FOIA),

  State and local disclosure laws, and

  Use in civil litigation
- PCII cannot be used for regulatory purposes and can only be accessed in accordance with strict safeguarding and handling requirements.

http://www.ocp.virginia.gov/Initiatives/CIP.cfm

Private Sector Engagement

In coordination with the previously mentioned initiatives the OCP CIP program works to engage private sector partners in the implementation of the VCIPRSP. The OCP has established relationships with the FBI's Infragard program which focuses on private sector outreach and awareness.

http://www.ocp.virginia.gov/Initiatives/CIP.cfm

Links of Interest

- National Infrastructure Protection Plan http://www.dhs.gov/files/programs/editorial_0827.shtm
- VCIPRSP http://www.ocp.virginia.gov/Initiatives/documents/VA_Plan.pdf
- IT Sector Specific Plan http://www.dhs.gov/xlibrary/assets/nipp-ssp-information-tech.pdf
- Communications Sector Specific Plan http://www.dhs.gov/xlibrary/assets/nipp-ssp-communications.pdf

http://www.ocp.virginia.gov/Initiatives/CIP.cfm

Mike McAllister
Critical Infrastructure Coordinator
804-692-2596
804-840-7837
Mike.McAllister@governor.virginia.gov

http://www.ocp.virginia.gov/Initiatives/CIP.cfm

Thank You!!

http://www.ocp.virginia.gov/Initiatives/CIP.cfm

Identity Theft Prevention Program

I don't have to implement an identity theft prevention program...or do I?

Steve Werby, VCU ISO

FTC Red Flags Rule

- Requires implementation of a written identity theft prevention program that detects warning signs of identity theft in connection with new and existing accounts

- Applies to financial institutions and creditors

But my agency isn't a financial institution!

- Financial institution – holds a transaction account belonging to a consumer
- Transaction account – account from which owner makes payments or transfers
- Creditor – regularly extends/renews/continues credit (permit deferred payments for a purchase)

Covered accounts

- Type 1 – consumer account designed to permit multiple transactions

- Type 2 – any other account for which there's reasonable foreseeable identity theft risk to customers or your organization

- VCU examples
  - Student installment payment plan accounts
  - Loan accounts
  - VCUCard (debit bank card via Wachovia)

How to comply

1. Identify relevant red flags
2. Implement procedures to detect red flags
3. If detected, respond to mitigate identity theft
4. Train employees
5. Keep the program current

Types of red flags

1. Suspicious account activity
2. Suspicious identifying information
3. Suspicious documents
4. Information from credit reporting agencies
5. Notices from other sources

When?

- Red Flags Rule issued November, 2007
- Effective January, 2008
- Compliance November 2008
  Compliance May 2009
  Compliance August 2009
  Compliance November 2009

Implementation

- Convene committee
- Develop policy (approved by BOV)
- Designate program administrator
- Develop communication and training plan
- Establish oversight and administration

Key points

- Red Flags Rule is flexible
- Consider your risk factors
- Don't forget your service providers
- Even if not required, consider implementing program

References

- FAQ:
  http://www.ftc.gov/bcp/edu/microsites/redflagsrule/faqs.shtml

- How-To Guide for Business:
  http://www.ftc.gov/redflagsrule

- 26 possible red flags (page 63774):
  http://ftc.gov/os/fedreg/2007/november/071109redflags.pdf

- VCU Identity Theft Prevention policy:
  http://infosecurity.vcu.edu/docs/identity-theft-prevention-policy.pdf

Virginia Information Technologies Agency

Commonwealth Information Security Council

Steve Werby
VCU & COV IS Council

Encryption Committee

Contact:

smwerby@vcu.edu

Initial Risk Assessment Process

Eric Taylor – Information Security Architect

Agenda

- Over view
- Objective
- The IRAP Process
- The IRAP Consumer
- Summary

IT Risk Assessment

- **The purpose of IT risk management is to determine risks to IT systems, prioritize those risks and plan and respond to those risks in the COV that could result in material or significant negative impacts on essential business functions and the mission of agencies.**
- **The process of identifying the vulnerabilities, threats, likelihood of occurrence, potential loss or impact, and theoretical effectiveness of security measures. Results are used to evaluate the level of risk and to develop security requirements and specifications.**
- **Defined in IT Risk Management Guideline (SEC506-01)**

What is the IRAP?

- **Initial Risk Assessment Process (IRAP) - information security risk assessment on preliminary requirements or a security problem set.**
  - **Measures application/project requirements against policy and provides functional adjustments. Focuses on early assessment of the application's or Infrastructure component's requirements for confidentiality, integrity and availability (CIA)**
  - **Decisive account of the risk to IPT infrastructure from a requested implementation or change within the environment.**
  - **Documentation with recommended actions or risk acceptance.**
- **Scope – Enterprise Environment, SLA, RFS projects**
- **IRAP – is not a full Risk Assessment.**

Objective

- The objective of performing risk management is to enable the organization to accomplish its mission;
  - by better securing the IT systems that store, process, or transmit organizational Information;
  - by enabling management to make well-informed risk management decisions to justify the expenditures that are part of an IT budget;
  - by assisting management in authorizing (or accrediting) the IT systems on the basis of the supporting documentation resulting from the performance of risk management.
- Address security concerns for the Partnership Infrastructure

Process Interaction

2009-08-13

Who the IRAP starts?

- **RFS**
  - **If a proposed solution is determined a security risk to the enterprise environment**
- **COV Policy Exemption**
  - **Note: This request is for an exception(s) to a component of the Commonwealth policy and/or standard(s) and approval of this request does not in any way address the feasibility of operational implementation. You are encouraged to check with your technical support staff prior to submitting this request.**
  - **Enterprise risk from an approved COV Policy Exemption**
- **Security Problem**
  - **An issues is identified that could pose a security risk.**
- **The IRAP will be completed by the "Governance, Risk and Compliance (GRC) Team" or a Qualified Security Professional**

Completing the IRAP

- **The IRAP document**
  - **Summary – objective of the security issue**
  - **Scope – It is primarily concerned with defining and controlling what is or is not included in the IRAP**
  - **Current Environment**
    - **Provides a brief general technical description of the system. Discuss any environmental factors that raise special security concerns and document the physical location of the system.**
    - **Provide a network diagram or schematic to help identify, define, and clarify the system boundaries for the system, and a general description of the system.**

Completing the IRAP – Con't

- **Risk Profile**
  - **Provide a general technical description of the threats and vulnerabilities that product X or change X poses on the current environment. This should include at least:**
    - **any dependencies or prerequisites;**
    - **access required (local or remote);**
    - **compromised systems;**
    - **threat agents.**
  - **This information should match the Risk Matrix. Provide documented best practices or standards that should be referenced properly.**

Completing the IRAP – Con't

- **Risk Matrix**
  - **Threat & Vulnerability Description -** A threat is an event, process, activity, or action that exploits a vulnerability to attack an asset. Vulnerability is a weakness which a threat will exploit to attack the assets.
  - **Business Impact (H, M, L) -** Derived from the level of data sensitivity and business mission. Additionally, if submitted, a business impact assessment (BIA) is considered.
- **Likelihood (H, M, L) -** Corresponds to likelihood of a threat exploiting a vulnerability
- **Existing Controls -** Controls are safeguards that reduce the probability that a threat will exploit a vulnerability to successfully attack an asset. Identify those safeguards that are currently implemented, and determine their effectiveness in the context of the current analysis.
- **Summary Risk Level (H, M, L) –** the combination of the Business Impact and likelihood.

Likelihood	High	Low	Medium	Hi
	Medium	Low	Medium	Medium
	Low	Low	Low	Low
		Low	Medium	High
		Business Impact		

- **Mitigation -** Identification of additional safeguards to minimize the threat exposure and vulnerability exploitation for each threat/vulnerability
- **Residual Risk (H, M, L) -** The potential for the occurrence of an adverse event after adjusting for the impact of implementing mitigation safeguards.

Completing the IRAP – Con't

- **Corrective actions and Recommended controls**
  - **This area is used to provide a solution to the problem and ask the IRAP consumer to accept the recommendations**
  - **If corrective actions are not taken and the residual risk is medium or high then a risk acceptance statement is required**
- **Conclusion – Summary statement showing cumulative risk**
- **Risk Acceptance Agreement**
  - ***Not every IRAP will require signatures***
  - **If IRAP consumer decides the risk is not worth or justified to implement the corrective actions.**
  - **Signature is required block.**
- **References**
  - **COV Policies or Standards**
  - **Supporting Documentation**
  - **Vendor or Industry best practices**
- **Addendum - Risk definitions**

The IRAP consumer

- **The intended audience of the IRAP depends on the situation the risk pertains to:**
  - **Infrastructure, strategic goals, adherence to contract – NG PSO**
  - **Ability to provide SLA – VITA SMO**
  - **Application or Agency issue – Agency AOM to ISO**
- **The IRAP consumer will either allow NG to implement the corrective actions or sign the risk acceptance.**
- **The IRAP will be filed with NG Program Security Office – GRC Team, for future reference.**

Summary

- **Document The Risk**
  - **Informed decision**
  - **Current Environment**
  - **Risk Profile**
  - **Recommended Corrective Actions and Controls Or Risk Acceptance**
  - **Move on….**

What is Information Security?
Managing Risk

Questions

Virginia Information Technologies Agency

2009 COV Security Standard Significant Requirements Changes

John Green
Deputy Chief Information Security Officer

Overview

- Many changes & tweaks throughout the document
- Some minor, some significant
- This presentation focuses on significant or noteworthy additions or changes
- Not intended as a roadmap for all changes
- Compliance date of January 1, 2010

1. Introduction

- Acknowledge that information is the asset requiring protection
- Information can be contained on many types of media
- A holistic information security program must address all
- Changed “Information Technology” (IT) to “Information” throughout **most** of the Standard

2. Risk Management

- This section now contains the requirements associated with Key Roles & Responsibilities that previously resided in the Security Policy

- Outlines Agency Head –> IT System Users

- Note: Avoiding Potential Conflicts of Interest: "The ISO <u>should</u> report directly to the agency head where practical and <u>should not</u> report to the CIO."

2.5 Sensitive IT System Inventory and Definition

- IT Systems can be created very quickly, i.e. Microsoft Sharepoint
- Do we inventory, classify, assess and audit 10's or 100's of IT systems when they all look the same?
- New: "Note: Data and homogeneous systems, belonging to a single agency, that have the same technical controls and account management procedures, may be classified and grouped as a single set of data or systems for the purpose of inventory, data classification, risk assessments, and security audits, etc"

3. IT Contingency Planning

- 3.4 IT System and Data Backup and Restoration
  - Originally contained provisions for planning & operation of backups as well as protection
  - Backups are useless if they can't be restored

- New: "3.4.2 #11. Document and exercise a strategy for testing that IT system and data backups are functioning as expected and the data is present is a usable form."

- New: "3.4.2 #12. For systems that are sensitive relative to availability, document and exercise a strategy for testing disaster recovery procedures, in accordance with the agency's Continuity of Operations Plan."

4. Information Systems Security

- Acknowledge that applications have become the attack vector of choice for hackers
- The Commonwealth needs to focus on the security of applications being developed & those already operationally deployed
- 4.7 Application Security
  - Overall enhancements to Security Design & Application Development requirements

4.7.2 Application Planning

- NEW: "4.7.2 #4. Security Design – Use the results of the Data Classification process to assess and finalize any encryption, authentication, access control, and logging requirements. When planning to use, process or store sensitive information in an application, agencies must address the following design criteria:

  a. Encrypted communication channels shall be established for the transmission of sensitive information;

  b. Sensitive information shall not be visibly transmitted between the client and the application; and

  c. Sensitive information shall not be stored in hidden fields that are part of the application interface."

4.7.2 Application Development

- NEW: "4.7.2 #5. Authentication – Application-based authentication and authorization shall be performed for access to data that is available through the application but is not considered publicly accessible."

- NEW: "4.7.2 #6. Session Management – Any user session created by an application shall support an automatic inactivity timeout function."

- NEW: "4.7.2 #7. Data storage shall be separated wither logically or physically, from the application interface (i.e., design two or three tier architectures where possible)."

4.7.2 Production & Maintenance

- Protecting sensitive data served to the public
  - NEW: "4.7.2 #14. Internet-facing applications classified as sensitive shall have periodic vulnerability scans run against the application and supporting server infrastructure, and always when any significant change to the environment or application has been made. Any remotely exploitable vulnerability shall be remediated immediately. Other vulnerabilities should be remediated without undue delay.

Note: It is strongly recommended that agencies adopt application vulnerability scanning and remediation for all internal sensitive applications as well."

4.8 Wireless Security

- Entirely new section
- Drew the most comments in its original form on ORCA
- Final form acknowledges:
  - Heightened risk of internal WLANS
  - Need for public access, open hotspots
  - Wireless bridging devices for campus situations
- Will be refined over time

4.8.2 #1 WLAN Connectivity on the COV Network

- NEW: Wireless LAN (WLAN) Connectivity on the COV Network

The following requirements shall be met in the deployment, configuration and administration of WLAN infrastructure connected to any internal Commonwealth of Virginia network.

a. Client devices connecting to the WLAN must utilize two-factor authentication (i.e., digital certificates);
b. WLAN infrastructure must authenticate client devices prior to permitting access to the WLAN;
c. LAN user authorization infrastructure (i.e., Active Directory) must be used to authorize access to LAN resources;
d. Only COV owned or leased equipment shall be granted access to an internal WLAN;
e. All WLAN communications must utilize a secure encryption algorithm that provides an automated mechanism to change the encryption keys multiple times during the connected session and provide support for secure encryption protocols (i.e., the Counter Mode with Cipher Block Chaining Message Authentication Code Protocol encryption mechanism based on the Advanced Encryption Standard cipher);
f. Physical or logical separation between WLAN and wired LAN segments must exist;
g. All COV WLAN access and traffic must be monitored for malicious activity, and associated event log files stored on a centralized storage device;
h. Configuration and security data associated with the WLAN must not be provided to unauthenticated devices. For example, SSID broadcasting will be disabled; and
i. WLAN clients will only permit infrastructure mode communication.

4.8.2 #2 WLAN Hotspot

- NEW: WLAN Hotspot (Wireless Internet)

2. When building a wireless network, which will only provide unauthenticated access to the Internet, the following must be in place:

a. WLAN Hotspots must have logical or physical separation from the agency's LAN;
b. WLAN Hotspots must have packet filtering capabilities enabled to protect clients from malicious activity;
c. All WLAN Hotspot access and traffic must be monitored for malicious activity, and log files stored on a centralized storage device; and
d. Where COV clients are concerned, WLAN clients will only permit infrastructure mode communication.

4.8.2 #3 Wireless Bridging

- NEW: Wireless Bridging

  3. The following network configuration shall be used when bridging two wired LANs:

    a. All wireless bridge communications must utilize a secure encryption algorithm that provides an automated mechanism to change the encryption keys multiple times during the connected session and provide support for secure encryption methods (i.e., the Counter Mode with Cipher Block Chaining Message Authentication Code Protocol encryption mechanism based on the Advanced Encryption Standard cipher);
    b. Wireless bridging devices will not have a default gateway configured;
    c. Wireless bridging devices must be physically or logically separated from other networks;
    d. Wireless bridge devices must only permit traffic destined to traverse the bridge and should not directly communicate with any other network;
    e. Configuration and security data associated with the WLAN must not be provided to unauthenticated devices. For example, SSID broadcasting will be disabled; and
    f. Wireless bridging devices must not be configured for any other service than bridging (i.e., a wireless access point).

5. Logical Access Controls

- Significant effort to reorganize Section 5.2 Account Management to be more clear & concise.
- Worth noting:
  - "CHANGE 5.2 #9 Prohibit the use of shared accounts on all IT systems. Those systems residing on a guest network are exempt from this requirement."
  - "CHANGE 5.2 #10 Prohibit the display of the last logon user ID on multi-user systems. Desktop and laptop systems assigned to a specific user are exempt from this requirement."
  - "CHANGE 5.2 #17 Prohibit the granting of local administrator rights to users. An Agency Head may grant exceptions to this requirement for those employees whose documented job duties are primarily the development and/or support of IT applications and infrastructure. These exception approvals must be documented annually and include the Agency Head's explicit acceptance of defined residual risks."

6.2 Data Protection

- Addressing the realities of contractors & consultants
  - "CHANGE 6.2.2 #3 Prohibit the storage of any Commonwealth data on non-COV issued computing devices. This prohibition, at the agency's discretion need not apply to Internet-facing web sites serving non-sensitive data. Agency contactors may store non-sensitive COV data for the execution of the agency contract. This requirement is due to records retention and Freedom of Information Act (FOIA) complexities, as well as the associated information security risks."

- Allowing the business of serving our citizens
  - "CHANGE 6.2.2 #5 Prohibit the connection of any non-COV owned data storage media or device to a COV-owned resource, unless connecting to a guest network or guest resources. This prohibition, at the agency's discretion need not apply to an approved vendor providing operational IT support services under contract."

6.3 Encryption

- Encouraging the creation of security zones
  - CHANGE 6.3.2 #3 Require encryption for the transmission of data that is sensitive relative to confidentiality or integrity over non-Commonwealth networks or any publicly accessible networks, or any transmission outside of the data's broadcast domain; however, digital signatures may be utilized for data that is sensitive solely relative to integrity.

6.4 Protection of Sensitive Information on Non-Electronic Media

- NEW: 6.4.2 Recommended Best Practices

  These recommendations apply to non-electronic media:

  1. While in use, limit access based on a need to know basis by physically controlling access. For example, sensitive documents printed to a global printer should be retrieved without delay.
  2. While not in use, store in a secure location with appropriate physical controls.
  3. When no longer needed, securely destroy using appropriate destruction methods such as erasing white or black boards and shredding paper.

9.3 Information Security Monitoring & Logging

- CHANGE: 9.3.2 #2 Enable event logging on all IT systems. At a minimum, logs will include:
  - The event;
  - The user ID associated with the event; and
  - The time the event occurred

- **Note**: Examples of events might include logons, invalid access attempts or data deleted, changed or added.

Comments & Questions

- Commonwealth Security & Risk Management welcomes ongoing comments & questions:

CommonwealthSecurity@vita.virginia.gov

Virginia Information Technologies Agency

2009
Commonwealth Security Annual Report

Benny Ambler
Enterprise Risk, Assurance & Standards Manager

§ 2.2-2009

§ 2.2-2009. (Effective until July 1, 2008) Additional duties of the CIO relating to security of government information.

C. The CIO shall report to the Governor and General Assembly by December 2008 and annually thereafter, those executive branch and independent agencies and institutions of higher education that have not implemented acceptable policies, procedures, and standards to control unauthorized uses, intrusions, or other security threats. For any executive branch and independent agency or institution of higher education whose security audit results and plans for corrective action are unacceptable, the CIO shall report such results to the (i) Information Technology Investment Board, (ii) affected cabinet secretary, (iii) Governor, and (iv) Auditor of Public Accounts. Upon review of the security audit results in question, the Information Technology Investment Board may take action to suspend the public bodies information technology projects pursuant to subdivision 3 of § 2.2-2458, limit additional information technology investments pending acceptable corrective actions, and recommend to the Governor any other appropriate actions.

Explanation

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates
Agency XYZ	Yes	10	Yes	Yes	Yes

Acronyms:

ISO: Information Security Officer
IS: Information Security
CAP: Corrective Action Plan
CISO: Chief Information Security Officer of the Commonwealth

ISO Designated: The Agency Head has

Yes - designated an ISO with the agency within the past two years
No - NOT designated an ISO for the agency since 2006
Expired –designated an ISO more than 2 years ago or the designated ISO is no longer with the agency

Attended IS Orientation:

The number indicates agency personnel that have attended the optional Information Security Orientation sessions within the last 2 years. Their attendance indicates they are taking additional, voluntary action to improve security at their agency akin to "Extra Credit!"

Explanation – Continued

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates
Agency XYZ	Yes	10	Yes	Yes	Yes

Security Audit Plan Received: The Agency Head has

Yes - submitted a Security Audit Plan for the period of fiscal year 2009 - 2011 for systems classified as sensitive based on confidentiality, integrity or availability

No - not submitted a Security Audit Plan since 2006

Exception – submitted an exception on file with VITA to allow time for developing the Security Audit Plan & the CISO has approved

Expired –submitted a Security Audit Plan on file that does not contain the current three year period FY 2009 – FY 2011

Pending –submitted a Security Audit Plan that is currently under review

Corrective Action Plans Received: The Agency Head or designee has

Yes - submitted an adequate Corrective Action Plan or notification of no findings for Security Audits scheduled to have been completed

Some - submitted an adequate Corrective Action Plan or notification of no findings for some, but NOT all Security Audits scheduled to have been completed

No - NOT submitted any adequate Corrective Action Plans or notification of no findings for Security Audits scheduled to have been completed

Not Due - not had Security Audits scheduled to be completed

N/A - not submitted a Security Audit Plan so not applicable

Pending –submitted a Corrective Action Plan that is currently under review

Explanation – Continued

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates
Agency XYZ	Yes	10	Yes	Yes	Yes

Quarterly Updates: The Agency Head or designee has

Yes - submitted adequate quarterly status updates for all corrective actions resulting from Security Audits previously conducted by or on behalf of the agency

Some - submitted adequate quarterly status updates for some corrective actions resulting from Security Audits previously conducted by or on behalf of the agency

No - not submitted ANY quarterly status updates for some corrective actions resulting from Security Audits previously conducted by or on behalf of the agency

Not Due - no open Security Audit findings

N/A - not submitted a Security Audit Plan or a Corrective Action Plan that was due

Pending - submitted quarterly status update that is currently under review

FAQ!

What should an agency do if they conduct a Security Audit that results in no findings?

In the event that a Security Audit was performed and there were no findings and, therefore, no Corrective Action Plan is due, the Agency Head should notify Commonwealth Security via email or letter stating what audit was conducted and that there were no findings.

What is the cutoff date to submit documentation for the Commonwealth Security Annual Report?

October 31, 2009

Secretariat: Administration

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAP's Received	Quarterly Updates
Human Rights Council	Yes	0	No	N/A	N/A
Dept. of General Services	Yes	0	Expired	No	N/A
Dept. of Human Res. Mgmt	Yes	0	Expired	No	N/A
Dept. Min. Bus. Enterprise	Yes	1	Pending	Pending	N/A
Employee Dispute Resolution	Yes	3	Expired	Not Due	Not Due
Compensation Board	Yes	1	Expired	No	N/A
State Board of Elections	Yes	1	Expired	No	N/A

Secretariat: Agriculture & Forestry

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAP's Received	Quarterly Updates
Dept. of Forestry	Yes	1	Pending	Not Due	Not Due
Va. Dept. of Ag. & Cons. Serv.	Yes	30	Yes	Yes	Yes

Secretariat: Commerce & Trade

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAP's Received	Quarterly Updates
Dept of Business Assistance	Yes	2	Yes	Not Due	Not Due
Board of Accountancy	Yes	0	Yes	Yes	Not Due
Dept. of Housing & Community Development	Yes	1	Yes	Some	Some
Dept. of Mines, Minerals & Energy	Yes	1	Yes	Yes	Yes
Dept. of Labor & Industry	Yes	3	No	N/A	N/A
Dept. of Professional & Occupational Regulation	Yes	1	Yes	Not Due	Not Due
Tobacco Indemnification Commission	Yes	1	No	N/A	N/A
Va. Employment Commission	Yes	2	Expired	Some	Yes
Va. Economic Development Partnership	Yes	0	No	N/A	N/A
Va. Housing Development Authority	Expired	1	No	N/A	N/A
Va. National Defense Industrial Authority	Yes	0	No	N/A	N/A
Va. Resources Authority	No	0	No	N/A	N/A
Va. Racing Commission	Yes	1	Yes	Pending	Pending

Secretariat: Education

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAP's Received	Quarterly Updates
Dept. of Education	Yes	2	Pending	No	N/A
Frontier Culture Museum of Va.	Yes	0	No	N/A	N/A
Gunston Hall	Yes	0	No	N/A	N/A
Jamestown - Yorktown Foundation	Yes	1	Pending	Pending	N/A
Library of Va.	Yes	1	Yes	Not Due	Not Due
State Council of Higher Education for Va.	Yes	0	Pending	N/A	N/A
Science Museum of Va.	Yes	1	Yes	N/A	N/A
Va. Commission for the Arts	Yes	0	Yes	Not Due	Not Due
Va. Museum of Fine Arts	Yes	2	Pending	Yes	No

Secretariat: Education (Cont'd)

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAP's Received	Quarterly Updates
Christopher Newport University	Yes	0	Pending	No	N/A
George Mason University	Yes	1	Yes	Some	Yes
James Madison University	Yes	1	Yes	Yes	Pending
Longwood University	Yes	1	Pending	Yes	Yes
Norfolk State University	Yes	2	Yes	No	N/A
Old Dominion University	Yes	0	Pending	Yes	Yes
Radford University	Yes	0	Yes	Yes	Yes
University of Mary Washington	Yes	1	Yes	Pending	Not Due
Va. Community College System	Yes	43	Yes	Yes	Yes
Virginia Military Institute	Yes	0	Pending	No	N/A
Virginia State University	Pending	3	Yes	Not Due	Not Due

Secretariat: Finance

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAP's Received	Quarterly Updates
Dept. of Accounts	Yes	4	Yes	Yes	Not Due
Dept. of Planning & Budget	Yes	1	Yes	No	N/A
Dept. of Taxation	Yes	0	Yes	Some	Some
Dept. of Treasury	Yes	3	Yes	Some	Some

Secretariat: Health & Human Resources

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAP's Received	Quarterly Updates
Dept. of Health Professions	Yes	2	Yes	Not Due	Not Due
Dept. of Medical Assistance Services	Yes	4	Yes	Yes	Yes
Department of Behavioral Health and Developmental Services ~~DMHMRSAS~~	Yes	22	Yes	Some	Some
Dept. of Rehabilitative Services	Yes	0	Pending	Pending	N/A
Dept. of Social Services	Yes	1	Expired	No	N/A
Virginia Foundation for Healthy Youth ~~TSF~~	Yes	1	No	N/A	N/A
Va. Dept. for the Aging	Yes	0	Yes	Not Due	Not Due
Va. Dept. of Health	Yes	3	Yes	Yes	Yes

Secretariat: Natural Resources

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAP's Received	Quarterly Updates
Dept. of Conservation & Recreation	Yes	2	Yes	Yes	Yes
Dept. of Environmental Quality	Yes	4	Yes	Yes	Yes
Dept of Game & Inland Fisheries	Yes	2	Expired	Some	No
Dept. of Historic Resources	Yes	2	Expired	No	No
Marine Resources Commission	Yes	3	Yes	Yes	Yes
Va. Museum of Natural History	Yes	1	No	N/A	N/A

Secretariat: Public Safety

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAP's Received	Quarterly Updates
Alcoholic Beverage Control	Yes	4	Yes	Yes	Yes
Commonwealth's Attorney's Services Council	Yes	0	No	N/A	N/A
Dept. of Criminal Justice Services	Yes	2	Yes	Not Due	Not Due
Dept. of Fire Programs	Yes	2	Yes	Not Due	Not Due
Dept. of Forensic Science	Yes	1	Expired	No	N/A
Dept. of Juvenile Justice	Yes	3	Yes	No	N/A
Dept. of Military Affairs	Expired	1	No	N/A	N/A
Dept. of Corrections	Yes	2	Expired	Some	No
Dept. of Correctional Education	Yes	1	Yes	Not Due	Not Due
Dept. of Veterans Services	Yes	0	Pending	N/A	N/A
Va. Dept. of Emergency Management	Yes	2	No	N/A	N/A
Va. State Police	Yes	2	Yes	Yes	Not Due

Secretariat: Technology

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAP's Received	Quarterly Updates
The Ctr for Innovative Tech.	Yes	1	Expired	No	N/A
Va. Info. Technologies Agency	Yes	30	Yes	Not Due	Not Due

Secretariat: Transportation

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAP's Received	Quarterly Updates
Dept. of Motor Vehicles	Yes	2	Yes	Not Due	Not Due
Dept. of Aviation	Yes	3	No	N/A	N/A
Dept. of Rail & Public Trans.	Yes	0	Yes	Not Due	Not Due
Motor Vehicle Dealers Board	Yes	0	Pending	N/A	N/A
Va. Dept. Of Transportation	Yes	5	Yes	Pending	Pending

Independent Branch Agencies

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAP's Received	Quarterly Updates
Indigent Defense Commission	Yes	4	Expired	Some	Not Due
State Lottery Dept.	Yes	0	Pending	N/A	N/A
State Corporation Commission	Yes	3	Yes	Not Due	Not Due
Va. College Savings Plan	Yes	3	Yes	No	N/A
Va. Office for Protection & Advocacy	Yes	1	Exception	Exception	Not Due
Va. Retirement System	Yes	2	Yes	No	N/A
Va. Workers' Compensation Commission	Yes	3	Exception	Exception	Not Due

Others

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAP's Received	Quarterly Updates
Office of the Governor	Yes	1	Exception	Exception	Not Due
Office of the Attorney General	Yes	0	Yes	Not Due	Not Due

Virginia Information Technologies Agency

Exceptional Exception Processing

Bob Baskette:
CISSP-ISSAP CCNP/CCDP RHCT
Commonwealth Security Architect

The Exception Process

- The Exception Request form is used to document the Risk associated with not adhering to the Security requirements and guidance stipulated in the Commonwealth of Virginia Security Policy, Standard, and Guidelines.
- The information provided on the form will be used by the COV Agency Head and the COV CISO to evaluate the Risk and Controls available to mitigate the Risk.
- The Exception Request should be submitted by the COV Agency ISO, the ISO's delegated contact, or the Business Owner. The Exception Request must be submitted by a COV employee.

Contact Section

- *This section provides the contact information for any additional information*

- **Agency Name:** Commonwealth of Virginia - Department of Examples and Presentations (007)

- **Contact for Additional Information:** Jon Dough, ISO DEAP (804)555-1212

Subject of Exception

- **Requirement to which an exception is requested**: The Commonwealth of Virginia Department of Examples and Presentations is requesting an exception to Section 5.2.2.17 of the Commonwealth of Virginia Information Technology Resource Management SEC 501-01 Security Standard. Require that local administrator rights, or the equivalent on non-Microsoft Windows based IT systems, be granted only to authorize IT staff.

1. Provide the Business or Technical Justification:

- Cathy Crayon (Graphic Artist/Promotions) and Billy Bean (Business Application Analyst) require Local Administrative rights to the end-user computer systems listed in Section 2 of this request. Cathy Crayon's position requires the installation of graphics software and fonts to support the creation of presentations for DEAP. Billy Bean's position requires the development and installation of database and accounting software to support the Account Receivable functions of DEAP. Both positions are required to install new software and update existing software at irregular intervals that cannot be practically supported by the existing COV-Partnership personnel.

2. Describe the scope including quantification and requested duration

- The following list of IT users or groups (*if the duties requiring Local Administrative privileges are role-based*) requires both Local Administrator and regular user accounts on the following PCs:
  - Cathy Crayon cathy.crayon@deap.virginia.gov
  - Billy Bean billy.bean@deap.virginia.gov

- **Duration: One Year**

3. Describe all associated risks:

Local Administrator accounts have complete and unrestricted access to the computer system hosting the Local Administrator account. The risks associated with a Local Administrator account include, but are not limited to the following:

- Installation of unauthorized, malicious, or non-licensed software
- Disablement of security or system monitoring software
- Alteration of system configuration settings or security logging facilities
- Escalation of privilege on the local computer system when not required

4. Identify the controls to mitigate the risks:

Individuals who are granted this privilege must be trusted to use the privilege in a responsible manner. The following controls will help mitigate the risks imposed by the presence of a Local Administrator account:

- The use of two separate accounts, one for Local Administrative functions and one for daily system usage as required in SEC501-01, Section 5.2.2 #16.
- Local system anti-virus software installed with the automatic update service enabled
- Security awareness training provided to the user at least once a year
- Signed acceptance of an acceptable use policy by the user at least once a year
- Review of applications installed on the system and Local system log file reviews conducted at least once every 60-days

5. Identify any residual risks:

Local Administrator accounts have complete and unrestricted access to the computer system hosting the Local Administrator account. This unrestricted access to the local computer system will limit the effectiveness of the controls referenced in Section 4. The unmitigated risks associated with a Local Administrative account include, but are not limited to the installation of unauthorized software, non-licensed software, malicious code, and other unauthorized activities that may go undetected between the local system log file review periods potentially compromising the entire network. Any file installed with the Local Administrator account could potentially contain a zero-day exploit that would not be detected or mitigated by the existing anti-virus software. If the zero-day exploit is a key-logging program the data entered into that local system could be exposed to malicious individuals resulting in the theft of Commonwealth of Virginia information or Virginia citizen Personal Identifiable Information granted to the Commonwealth of Virginia. In addition, the Local Administrator account will have full access to modify or delete the local system log files, thereby limiting the integrity of the information contained in the local system log files.

Submitting the Exception

1. Email the request to CommonwealthSecurity@vita.virginia.gov and CC your Agency Head in the email to document the Agency Head's approval.
2. Have your Agency Head sign the request and fax it to 804-416-6359
3. Have your Agency Head sign the request and mail it to: VITA Commonwealth Security, 11751 Meadowville Lane, Chester VA 23836

Final Thoughts

- Each Exception Request will only be valid for a maximum of 12-months.
- Each Exception Request must provide information on the remediation process to be used to eliminate the need for additional exception requests.
- Local Admin Rights exceptions (SEC 501-01 Section 5.2.2.17) require two accounts. One for daily use and one for Local Admin Rights (SEC 501-01 Section 5.2.2.16)

Questions???

For more information, please contact:
CommonwealthSecurity@VITA.Virginia.Gov

Thank You!

Virginia Information Technologies Agency

Keys to the Kingdom: Encryption Mechanics and Key Management

Bob Baskette:
CISSP-ISSAP CCNP/CCDP RHCT
Commonwealth Security Architect

Cryptography Basics

- Use of deception and mathematics to render data unintelligible through the transformation of data into an unreadable state and to ensure that a message has not been altered in transit.
- Protects transmitted information from being read and understood by anyone except the intended recipient.
- Cryptography ensures integrity, confidentiality, authentication, authorization, and using certain mechanisms non-repudiation
- Cryptography does not support availability

Cryptography Basics Continued

- Cryptosystem
  - Set of transformations from a message space to ciphertext space
  - Includes the encryption algorithm, keys, and necessary software components and protocols.
- Cryptographic Algorithm
  - Step-by-step procedures used to encipher plaintext and decipher ciphertext
- Cryptoanalysis
  - Study of techniques for attempting to defeat cryptographic techniques

Cryptography Basics Continued

- Key = crypto-variable
  - Sequence that controls the operation of the cryptographic algorithm
  - Determines the behavior of the algorithm and permits reliable operations
  - Comprises a large sequence of random bits
- KeySpace
  - Range of values that can be used to construct a key
  - Used by the algorithm to generate new random keys
  - The total number of possible values of the keys in a cryptographic algorithm

Cryptography Basics Continued

- Clustering
  - Situation in which a plaintext message generates identical ciphertext when using the same algorithm but different crypto-variables or keys
- Collision
  - When a hash function generates the same output for different inputs
- Avalanche Effect
  - A minor change in the either the key or plaintext will have a significant change in the resulting cipher text

Steganography (Hidden-writing)

- Secret communication in which the existence of the message is hidden in another media type
- The contents of the message is not encrypted
- The least-significant bit of each word in an image can be used to encode a message with causing any significant change to the image
- Can be used to create digital watermarks (the addition of identification information into a file or document)

Initialization Vector

- Non-secret binary vector used to initialize the input algorithm for encryption
- Random values used to ensure patterns are not created during encryption
- Used with keys and does not need to be encrypted during distribution
- Increases security by introducing additional cryptographic variance and synchronize cryptographic equipment

Strength of Cryptosystem

- Specifies the difficulty of uncovering the algorithm or key (whichever one if kept private)
- Determined by:
  - The time and resources needed to break algorithm or key
  - Algorithm
  - Secrecy of key
  - Initialization vectors

Important elements of encryption:

- Use an algorithm without flaws
- Use a large key size
- Use all possible values within the keyspace
- Protection of the key

Kerckhoff's Law

- A cryptosystem should be secure even if everything about the system, except the key, is public knowledge
- Algorithm should be in the public domain to reduce the vulnerabilities in algorithm

Transposition/Permutation

- Process of re-ordering plaintext to hide the message
- Key is used to determine the positions the values are moved
- Rearranges the original bits, characters, or blocks of characters to hide message
- Used in Symmetric algorithms

Substitution

- Process of exchanging one letter or byte for another (Caesar Cipher, monoalphabetic cipher, subset of the Vigenere polyalphabetic cipher)
- Can be attacked by frequency analysis
- The frequency of characters shown in the use of the alphabet's letters in a particular language are used.
- Uses a key to dictate how the substitution should be performed.
- Used in Symmetric algorithms

Confusion

- Commonly carried out via substitution
- Mixing or changing the key values used during the repeated rounds of encryption
- Provides added complexity
- Pertains to making the relationship between the key and the resulting ciphertext as complex as possible to prevent the key from being recovered from the ciphertext

Diffusion

- Commonly carried out via transposition
- Takes place as individual bits of a block are scrambled through the block
- Mixing up the location of the plaintext throughout the ciphertext
- A single plaintext bit has influence over several ciphertext bits such that changing a plaintext bit should change many ciphertext bits
- Through transposition, the location of the first character of the plaintext may change several times during the encryption process

SP-Networks

- Process used in block ciphers to increase the strength
- SP is substitution and permutation
- Most block ciphers do a series of repeated SP actions to add confusion and diffusion
- S-Boxes handle the substitution
- Strong ciphers require Confusion and Diffusion
- Randomness of key and complexity of mathematical functions dictate level of Confusion and Diffusion

Monoalphabetic / Polyalphabetic Substitution Ciphers

- **Mono**
  - Substitution of one alphabet letter for another
- **Poly**
  - Use of several alphabets for substituting the plaintext
  - Resistant to frequency analysis
  - List plaintext above multiple alphabets
  - Use substitution row based on the number position of the letter in the plaintext word
- **Blais de Vigenere**
  - Polyalphabetic cipher developed for Henry III using a key word and 26/27 alphabets (each one off-set by one place)
  - Top-row used for the plaintext
  - First column uses to find the row based on the key.

Running Key Cipher

- Does not require an electronic algorithm
- Could use components of real world
- If implemented by real world objects = pre-define objects and list order of objects in a continuous stream of symbols
- The key is repeated for the same length as the plaintext input.
- Cipher uses text (from a book or other well-known source) to encrypt the plaintext
- Text is matched character for character with the plaintext
- Uses modulo 26 addition
- Eliminates periodicity (when substitution repeats)
- Can be attacked by exploiting redundancy of key

One-Time Pad = Vernam Cipher

- Technique where the key has the same length as the message
- Key is used to encipher one character of plaintext
- Key is truly random
- Implemented as a stream cipher using XOR function
- Decrypt by XOR function of ciphertext and key

One-Time Pad = Vernam Cipher

- Not practical for megabyte or gigabyte messages
- Each key letter is added modulo 26 to each letter of plaintext
- Uses principle of the Running Key using the numerical values of the letters and adding those to the value of the key.
- Considered unbreakable if:
  - Key is used only once and never used again (prevent pattern detection)
  - Key (pad) must be as long as plaintext message
  - Key (pad) must be securely distributed
  - Key (pad) must be truly random

Encryption Key Types

- Secret
  - Symmetric Encryption
    - Also known as
      - Private-key
      - Shared-key
- Session
  - Symmetric Encryption
    - Key used only for one transmission session
- Public
  - Asymmetric Encryption
- Quantum
  - Symmetric Encryption
  - Key sent using Quantum Mechanics

Symmetric Cryptography

- Can use either substitution or transposition
- Use of a single key for both encryption and decryption
- Security of encryption is completely dependent of protection of key
- Sender and receiver use the same key
- Will require a different key for each receiver to maintain Confidentiality
- Will require n(n-1)/2 keys

Symmetric Algorithm Advantages

- Very fast
- Secure method for confidentiality with large key size
- Algorithms can be implemented in hardware or software at little cost

Symmetric Algorithm Disadvantages

- Requires a separate secret key per communications partner (scalability)
- Challenge of Key management
  - Keys cannot be sent in the same channel as the messages
  - Requires some sort of out-of-band medium
- No support for non-repudiation, message integrity, access-control, or digital signatures

Symmetric Cryptography Methods

- **Stream**
- **Block**

Stream-based Symmetric Cryptography Methods

- Encryption on a bit-by-bit basis
- Each plaintext bit will be transformed into a different ciphertext bit each time it is encrypted
- Stream-based is usually implemented in hardware since they require more processing power
- Stream-based relies primarily on substitution
- Governed by the cryptosystem and controlled by the cipher key
- Key provides randomness to operation (prevents plaintext/ciphertext XOR revealing Key)

Block-based Symmetric Cryptography Methods

- Operates on blocks of bits or chunks of text
- Plaintext is divided into blocks of plaintext
- Each block is put through mathematical functions
- Uses combination of substitution and transposition (confusion and diffusion)
- Changing one plaintext bit could change half of the ciphertext bits
- Key determines what functions are applied to the plaintext and in what order (provides randomness to process)

Block-based Symmetric Cryptography Methods

- Usually stronger than Stream-based enciphering
- More expensive to implement
- Block-based is usually implemented in software
- Block Cipher Modes
  - Electronic Code Book (ECB)
  - Cipher Block Chaining (CBC)
  - Cipher Feedback (CFB)
  - Output Feedback (OFB)
  - Counter Mode (CTR)

Symmetric Algorithms

- Caesar
- Spartan scytale
- Enigma machine
- DES
- 3DES
- Blowfish
- Twofish
- IDEA
- RC4, RC5, RC6
- SAFER
- Serpent
- AES

DES = Data Encryption Standard = FIPS 46-3

- Based on the Lucifer algorithm 128-bit algorithm (IBM) (Harst Feistal)
  - Introduced complex mathematical equations and functions
  - NSA modified to use 64-bit key
  - The actual algorithm is DEA
  - DES is the standard
  - 1988 NSA stopped endorsing DES
- Uses a 56-bit key(length is 64-bit/8-bits used for parity)
- Symmetric block encryption algorithm
- Divides the message into blocks/operates one block at a time

DES = Data Encryption Standard = FIPS 46-3

- Operates on 64-bit blocks of data broken into 32-bit blocks
- Output is 64-bit blocks
- Key-Space is 2^56
- Uses transposition and substitution/controlled by key
- 16-round cryptographic system
- Can be implemented in hardware
- Uses confusion and diffusion to improve encryption

Block Modes of DES

- **ECB = Electronic Code Book Mode**
- **CBC = Cipher Block Chaining Mode**

ECB = Electronic Code Book Mode

- Native DES mode
- Operates like a code book by providing the combination of substitutions and permutations performed on the data block with the selection controlled by the Key
- Best used with small blocks of data
- Operates on input blocks independently
  - Operation is not order dependant since blocks encrypted independently
  - Will generate the same output block if two input blocks match since each block is encrypted with same key and therefore the same code book, which can expose the key or code book
  - Only good for short messages of less than 64-bits in length since this method does not provide enough randomness for use with large messages
- Uses 64-bit plaintext blocks
  - Will add padding if block is not 64-bits in length
  - Will divide block into two 32-bit blocks called Right and Left blocks
  - Bits are copied to produce two 48-bit blocks
  - Each 48-bit blocks will be XOR with 48-bit key

CBC = Cipher Block Chaining Mode

- Stronger than ECB
- Each block of text, the key, and the value based on the previous block are processes in the algorithm and applied to the next block of text
- Provides dependence between blocks and hides any patterns
- Each input block will generate a different output block
- Uses a randomly generated 64-bit initialization vector (IV) to XOR with the first block of plaintext to introduce randomness with the result encrypted with DES key to make it less predictable
  - IV xor Plaintext1 = ciphertext1
  - ciphertext1 xor plaintext2 = ciphertext2
- Different IV with same message will yield different encrypted message
- Operates with plaintext blocks of 64-bits
- Since this method chains blocks any error will be propagated

Stream Emulation Modes of DES

- DES is a block cipher that can simulate stream mode
- Block ciphers can be subject to problems of latency or delay in processing
- Used when data to be encrypted is a stream of continuous data instead of finite block
- Stream Mode Types:
  - **CFB = Cipher Feedback Mode**
  - **OFB = Output Feedback Mode**
  - **CTR = Counter Mode**

CFB = Cipher Feedback Mode

- Use to send large or continuous stream of data
- Example is terminal to terminal server (CBC operates on blocks of 64-bits) (stream data is usually 8-bits at a time)
- Cipher text is used as feedback into the key generation source to develop the next key stream
- Key and IV are used to generate the key-stream (random set of bits)
- Size of ciphertext needs to match size of plaintext (prevents patterns)
- Ciphertext generated by XOR of plaintext with key stream that has same number of bits as the plaintext and can propagate errors

CFB = Cipher Feedback Mode

- Input is separated into individual segments
  - 8-bit = size of one character
  - Each 8-bit are XOR inside a shift register
  - Once the XOR is complete the 8-bits are transmitted
- Can suffer failure if a single bit is corrupted or altered since all following data is corrupted
- Uses the same encryption process to encrypt and decrypt
- Need to use a new IV per message since message size is smaller enough for pattern matching

OFB = Output Feedback Mode

- Works well with small blocks of continuous stream data
- Values used to encrypt next block of plaintext come directly from the key-stream and not from the ciphertext
- Generates ciphertext by XOR plaintext with key stream
- Feedback is used to generate key stream
- Size of key-stream needs to match plaintext (prevents patterns)
- Key stream will vary
  - Errors are not propagated
  - Feeds the encrypted key-stream back into the shift register to create the next portion of the key-stream
- Does not chain the ciphertext
- Good for digitized video and digitized voice since the entire key-stream can be generated in advance and store for later use.

CTR = Counter Mode

- Used in high-speed applications (IPSec/ATM/802.11i) (packets often arrive out of order)
- Similar to Output Feedback Mode
- Uses an IV counter that increments for each plaintext block that needs to be encrypted
  - Ensures that each block is XORed with a unique key-stream value
- A counter (64-bit random data block) is used as the IV
  - The counter must be different for every block of plaintext
  - Counter will be incremented by 1
- Key-stream is separate from the data
- Ciphertext not used in the encryption process
- Can encrypt individual blocks in parallel
- Uses the same encryption process to encrypt and decrypt

3-DES Keying types

- Using 2 keys (DES-EEE2)
  - encrypt using Key1
  - encrypt using Key2
  - encrypt using Key1

- Using 2 Keys (DES-EDE2) (Allows backward compatibility with DES)
  - encrypt using Key1
  - decrypt using Key2 (used to jumble data/not decrypt data)
  - encrypt using Key1

- Using 3 keys (DES-EEE3)
  - encrypt using Key1
  - encrypt using Key2
  - encrypt using Key3

- Using 3 keys (DES-EDE3)
  - encrypt using Key1
  - decrypt using Key2 (used to jumble data/not decrypt data)
  - encrypt using Key3

AES = Advanced Encryption Standard

- Name of NIST standard
- Work began in 1998
- AES with a 256-bit key is considered by most to be the strongest algorithm
- Requirements outlined in FIPS PUB-197
  - Iterated block cipher (fixed block size of 128-bits)
  - Variable block length and key length that can be independently chosen as 128, 192, or 256 bits.
- Based on the Rijndael block Algorithm (developed by Belgian cryptographers Joan Daemen and Vincent Rijmen)
- Rijndael algorithm properities:
  - Resistance against all known attacks
  - Design simplicity
  - Code compactness and speed

AES Requirements

- **Layer Functions**
  - Nonlinear layer is the parallel application of S-Boxes that have optimum worst-case nonlinearity properties
  - Linear mixing layer provides a guarantee of a high diffusion of multiple rounds
  - Key addition layer is the XOR of the round key to the intermediate state
- Round Key is derived from the cipher key through a key schedule
  - Consists of a key expansion and Round key selection
  - Total number of Round key bits is equal to the block length x number of rounds +1
  - The Cipher key is expanded into an Expanded Key
  - Round keys are taken from the Expanded Key
    - 256-bit key and 256-bit block size = 14 rounds
    - 192-bit key and 192-bit block size = 12 rounds
    - 128-bit key and 128-bit block size = 10 rounds

Session Keys

- One approach to reduce the number of receiver keys used in a Symmetric encryption algorithm is to use a session key
- The session key is used for only one communication session between users
- Forms the basis for most encryption methods
- Use public-key cryptography to transmit a session key to the receiver
- Use timestamps to limit the lifetime of the session key (mitigate replay attacks)

Asymmetric Algorithms / Public Key

- Two keys linked mathematically, but would be mutually exclusive
- One key will encrypt/the other key would decrypt
- User generates two keys
  - Private Key that is kept secret and used to by receiver to decrypt messages
  - Public Key that can be sent to anyone and is used by sender to encrypt messages
- Important key properties:
  - Public key cannot decrypt message it encrypted
  - Private key cannot be derived from the public key
  - Message encrypted by one key can be decrypted by the other key
  - Private key must be kept secret
- Asymmetric algorithms are one-way functions

One-Way Functions

- Makes Asymmetric Cryptography possible
- A mathematical function that is easy to computer in one direction but difficult to compute in the reverse direction
- Function in easy direction provides encryption and digital signature verification and is performed with the public key
- Function in difficult direction provides decryption and signature generation and is performed with the private key
- Work factor for one-way function is the difference in time and effort that carrying out the one-way function in the easy direction takes compared to carrying out a one-way function in the difficult direction

Asymmetric-related terms

- **Trap-Door**
  - A secret mechanism that allows the one-way function to be easily reversed
  - Required to find the private key from the public key
- **Confidentiality**
  - Sender encrypts message with the receiver's public key
  - Only the receiver can decrypt the message
- **Non-repudiation**
  - Security service by which evidence is maintained so that the sender and the recipient of the data cannot deny having participated in the communications
  - Supported via public-key encryption and digital signatures
  - Sender encrypts the message with the sender's private key
  - The receiver opens with the sender's public key

Asymmetric Message Formats

- **Secure Message Format**
  - Encrypting a message with receiver's public key
  - Will provide confidentiality but not authentication or non-repudiation
- **Open Message Format**
  - Encrypting a message with the sender's private key
  - Will provide authentication and non-repudiation but not confidentiality

Asymmetric Key Considerations

- **Asymmetric Key Advantages**
  - Can send messages across unsecure mediums
  - No key management issues
  - Allows for non-repudiation and access-controls

- **Asymmetric Key Disadvantages**
  - Slower than Symmetric Key Cryptography
  - Ciphertext is much larger than the plaintext

Types of Asymmetric Algorithms

- RSA
- Elliptic curve Cryptosystems
- Diffie-Hellman
- El Gamal
- Digital Signature Algorithm
- Knapsack

RSA

- Rivest, Shamir, Adleman
- Public key algorithm
- Most popular for asymmetric algorithms
- Used in Microsoft, Apple, and Novell operating systems
- Can be used as key exchange protocol
  - System uses DES or AES to generate the symmetric key
  - Sends symmetric key encrypted with receiver's public key
- Provides authentication and key encryption

RSA

- Decryption based on the mathematical challenge of factoring the product of two large prime numbers to reveal the two prime numbers used to generate the specific large prime
- Public and private keys are functions of a pair of large prime numbers
- Most widely used public key algorithm and operates on blocks of text by C=P^e mod n
- Can be used for encryption, key exchange, and digital signatures
- Using its one-way function
  - Provides encryption and signature verification
  - Inverse direction provides decryption and signature generation

RSA attacks

- Brute-force
- Factoring prime numbers
- Timing attacks

Diffie-Hellman

- Developed to resolve the symmetric Key exchange problem by allowing the exchange or negotiate a symmetric key over non-secure medium
- First Asymmetric key agreement algorithm
  - Not key exchange (sending symmetric key encrypted with receiver's public key)
  - Provides for key distribution
  - Does not provide encryption or digital signature functions
- Does not provide message confidentiality
- Based on difficulty of calculating discrete logarithms in a finite field
- Sender uses sender's private key and receiver's public and the D-H algorithm to derive the shared value used to create instances of symmetric keys.

Diffie-Hellman

- Symmetric key used to encrypt data is created from only public information (public keys)
  - Uses two parameters which are both public
  - P = is a prime number
  - G = is the generator and is an integer less than P
- Running the public key through the DH algorithm will generate a common session key.
- D-H is vulnerable to Man-in-the-Middle attack
  - Does not perform authentication prior to public key exchange
  - Use digital signatures or digital certificates to perform authentication

El Gamal

- Extension of D-H
- Can be used for encryption, key exchange, and digital signatures
- Can provide message confidentiality and digital signatures
- Based on discrete logarithms in a finite field
- Very slow algorithm

Markle-Hellman Knapsack

- Based on the “knapsack problem”
- Mathematical dilemma based on the problem of having a set of items with fixed weights and determining which of these items can be added in order to obtain a given total weight
- Can be used for encryption and digital signatures
- Found to be insecure

Elliptic Curve Cryptography

- Has the highest strength per bit of key length
- Allows for shorter keys
- Fast and efficient (great for portable devices/small memory and processor)
- Will require fewer computational and memory requirements
- Suited to hardware applications such as smartcards and wireless devices
- Based on discrete logarithmic algorithms of elliptical curves
- Provides confidentiality, digital signatures, message authentication, and key management
- EC 160-bit key = RSA 1024-bit key

Key Strength Comparison

Asymmetric	vs.	Symmetric
512		64
1792		112
2304		128

PGP = Pretty Good Privacy

- Developed by Phil Zimmerman
- Freeware email security
- First widespread public key encryption system
- Can use RSA public key encryption for key management
- Can use IDEA symmetric cipher for bulk encryption
- Can use MD5 for integrity
- Can provide confidentiality, integrity, authentication, non-repudiation
- Passphrase used to encrypt user's private key on local host
- Does not use a CA to exchange keys / uses web of trust
- Key-ring = collection of public keys collected from other users

Quantum cryptography

- Uses physics to secure data = Also called Quantum Key Distribution = QKD
- QKD is a set of protocols, systems, and procedures used to create and distribute secret keys
- The quantum keys can be used with traditional cryptosystems to encrypt data
- QKD systems can only be used to generate keys and cannot be used as a stand-alone cryptosystem

Quantum cryptography

- Quantum Cryptography solves the issue of needing a secure channel to distribute secure keys because it allows secure key exchange based on the laws of physics
- Uses photon polarization to represent bit (vertical/horizontal/left/right)
- Each user must have the same polarization to binary mapping

Quantum cryptography

- **QKD uses to channels**
  - One channel is used to transmit the quantum key material via a single-photon light pulse
  - The other channel carries all messages including the cryptographic protocols
- **The basic law of QKD**
  - Once a photon has been observed, its state is changed
  - Allows for detection of eavesdropping

PKI = Public Key Infrastructure

- Establishes a level of trust within an environment
- ISO authentication framework that uses public key cryptography and X.509 standard
- Provides authentication, confidentiality, non-repudiation, and integrity of the messages exchanged
- Hybrid system of symmetric and asymmetric algorithms
- Assumes that the receiver's identity can be positively ensured via certificates and that an asymmetric algorithm will automatically carry out the key exchange

PKI Functions

- Identifies the users
- Create and distribute certificates
- Maintain and revoke certificates
- Distribute and maintain encryption keys

PKI Components

- Certificate authorities
- Registration authorities
- Certificate Repository
- Certificate revocation system
- Certificate Revocation List
  - Contains every certificate revoked by the CA
  - Most web browsers do not check the CRL for a CA.
- Key backup and recovery system
- Automatic key update
- Keys
- Users

PKI Digital Certificates

- Each person that wants to participate in PKI needs a digital certificate, which is a credential that contains the public key and other identifying information.
- The certificate must be signed by a Certificate Authority.
- Each individual must trust the same CA to exchange certificates.

Certificate Authority

- Acts as a notary by verifying a person's identity and issuing a certificate that vouches for a public key of the named individual
- Binds the individual to the public key
- Assumes liability for the authenticity of the individual
- Certificate is signed with the CA's private key

Digital Certificate Components

- Subject name
- Subject public key
- Name of the CA
- Serial number
- Version number
- Algorithm information
- Expiration date
- Signature of issuing authority

Certificate Authorities

- CA public key must be cross-certified with another CA
- X.509 standard defines the format for public key certificates
- Directory is simply a repository of public keys

Registration Authority

- Responsible for verifying an individual's identity
- Passes this information to the CA
- CA will then issue the certificate
- Performs certificate life-cycle management functions
- Acts as a broker between user and CA

Rules for Keys and Key management

- The key length should be sufficient to protect the message
- Keys should be stored and transmitted by secure means
- Keys should be extremely random and the algorithm should employ the full key space
- Keys lifetime should correspond to the sensitivity of the message
- Keys should be backed up or placed in escrow
- Keys should be properly destroyed at end of life

Key Recovery

1. Common Trusted Directories
2. Policy requiring all keys to be registered with the security department
3. Use steganography to hide passwords
4. Use a password wallet

Multi-party Key Recovery

- User would break private key into multiple parts and give each part to a trusted source with orders to only reveal that part in an emergency
- ANSI X9.17 was developed to address the need of Financial Institutions to transmit securities and funds securely
  - Based on the hierarchy of keys
  - Bottom used for data keys (DK) to encrypt/decrypt messages and are very short lived
  - Top used for the Master Key (KKM) to encrypt the data keys and have a longer life span

Cryptographic Attacks

- **Brute Force**
  - Exhaustive search of every possible key
- **Known Plaintext**
  - Attacker uses a copy of known plaintext (or parts of known plaintext) and ciphertext to attempt to determine the key
- **Chosen Plaintext**
  - Chose plaintext to be encrypted and the output is compare to the ciphertext
- **Adaptive Chosen Plaintext**
  - Adapt plaintext based on the results of the last Chosen Plaintext
- **Ciphertext only**
  - Attempt to decipher by analyzing several encrypted messages to discover key
  - Most common type of attack/hardest to achieve

Cryptographic Attacks

- **Chosen ciphertext**
  - Chose the ciphertext to decrypt and has access to the decrypted plaintext
- **Birthday attack**
  - Based on the mathematical birthday paradox that exists in standard statistics to find a collision in a hash algorithm.
  - Better than even chance of finding a match
  - Easier to find two matching values in a set of values than finding a specific match in the set.
  - Chance of finding a collision in a Hash algorithm is 2 ^ (Number of bits in message digest/2). 60-bits = 230 inputs.
- **Meet-in-the-middle**
  - Attack against Double DES
  - Brute-force attack against the plaintext
  - Encrypt known plaintext with all possible keys and create a table with all possible results
  - Attack has same work factor as DES

More Cryptographic Attacks

- **Differential Cryptanalysis**
  - Used on block cipher private key systems
  - Take two plaintext messages and follow changes made as they pass through S-boxes using same key
  - Analysis difference in ciphertext pairs to map probability values in keys
- **Side-Channel**
  - Review the facts and infer value of key
  - Detect power consumption for encryption and decryption
  - Intercept radiation emissions to determine how long process takes
- **Passive**
  - Eavesdropping and sniffing
  - Does not affect the protocol, algorithm, key, message

Wassenaar Agreement

Encryption Algorithms too dangerous to fall into terrorist state hands:

- Symmetric algorithms with key sizes over 56-bits
- Asymmetric algorithms that carry out factorization of an integer with key sizes over 512-bits (RSA)
- Asymmetric algorithms that compute discrete logarithms in a field with key sizes over 512-bits (El Gamal)
- Asymmetric algorithms that compute discrete logarithms in a group with key sizes over 112-bits (ECC)
- Exportation of most encryption tech is now allowed from the US (after technical review) except for those listed as terrorist states
- A technical review is not required if sent to foreign subsidiaries of US firm

Questions???

For more information, please contact:
CommonwealthSecurity@VITA.Virginia.Gov

Thank You!

Upcoming Events

Virginia Information Technologies Agency

2009 Information Security Awareness Tools

The Information Security Toolkit has been updated with new materials!

For printing cost estimates you can contact DMV's Damian McInerney at (804)367-0925 or email: damian.mcinerney@dmv.virginia.gov

Thank you DMV!

Virginia Information Technologies Agency

UPCOMING EVENTS! Future 2009 ISOAG's

From 1:00 – 4:00 pm at CESC

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

Tuesday **-** **October 6**

Wednesday - **November 18 @ SCC Building !**

Thank you, Blair Kirtley for organizing this!

Wednesday - **December 9**

Virginia Information Technologies Agency

Information Security System Association

ISSA meets on the second Wednesday of every month

- **DATE: Wednesday September 16th**
- **LOCATION: Hondo's, The Shoppes at Innsbrook 4024-C Cox Road, Glen Allen, VA (directions at http://www.hondosprime.com/get_directions.shtml)**
- **Topic: "Nine Proven Software Security Best Practices – Building Security in maturity Model (BSIMM)"**
- **TIME: 11:30 - 1:30pm. Presentation starts at 11:45 & Lunch served at 12.**
- **COST: ISSA members: $10 & Non-Members: $20**

Virginia Information Technologies Agency

11th Annual COVITS

Transparency, Participation & Collaboration

When: September 20-22, 2009

Where: Marriott – Williamsburg, Va.

Keynote Speakers
Aneesh Chopra, Federal Chief Technology Officer
&
Jerry Mechling, Harvard School of Government

Register at http://www.covits.org/

Govt employees: $99 / SWAM Members: $99 (Must be certified by the DMBE)

Virginia Alliance for Secure Computing and Networking (VASCAN)

VASCAN09
"Security in Lean Times"

When: October 5-6, 2009

Where: University of Virginia – Charlottesville, Va.

Registration: $100 for both conference days/$70 for one day (pre-registration required)

Hosted by: VASCAN (http://vascan.org)

(A block of rooms are being held for conference guests at the Cavalier Inn until September 14th)

UPCOMING EVENTS: MS-ISAC Webcast

National Webcast!

Thursday, October 8, 2009, 2:00 to 3:00 p.m.

Topic: In Conjunction with October Cyber Security Awareness Month

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/

UPCOMING EVENTS - CIO-CAO Mtg.

CIO-CAO Communications Meeting:

Tuesday, October 27

8:30 am – 9:00 am: Networking

9:00 am: Meeting start

Location: Perimeter Center
9960 Mayland Drive
Richmond, VA

FACTA Red Flag Requirements *NEW DATE

Implementation Date: **November** 1st, 2009

Announcement at: http://www.ftc.gov/opa/2009/07/redflag.shtm

Are you aware of the red flag requirements in the Fair and Accurate Credit Transactions Act (FACTA) of 2003?

Please read carefully as it is not only banks and financial institutions!

http://www.ftc.gov/bcp/edu/pubs/business/alerts/alt050.shtm

Virginia Information Technologies Agency

1st COV Information Security Conference

Date: November 2, 2009

Time: 8:30 a.m. – 4:30 p.m.

Where: Holiday Inn Koger Center, Richmond

Details and registration information to come!

Attendance limited to the first 95 who register.

(Small fee to state and local government attendees)

Any Other Business ??????

ADJOURN

THANK YOU FOR ATTENDING!!