Virginia Information Technologies Agency

Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

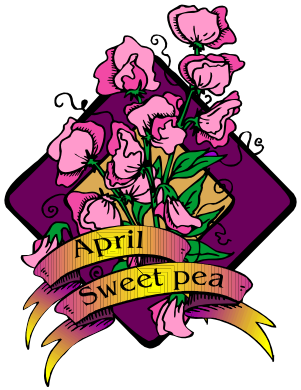
April 29, 2009


April


April
Diamond


Tax Time


W-2
Copy 2 to be filed with employ
Tax
1040
Department of the Treasury
U.S. Individual
APRIL


April
Sweet pea

ISOAG April 2009 Agenda

I.	Welcome and Opening Remarks	Peggy Ward, VITA
II.	System Access Request Application (SARA)	Jim Austin, VDOT
III.	Email Security - Messaging Encryption	Don Drew, VITA
IV.	Security Policy, Standards & Guidelines Processes	John Green, VITA
V.	Payment Card Industry Requirements	Peggy Ward, VITA
VI.	Administrative Measures – Security	Peggy Ward, VITA
VII.	Latte Larceny	Bob Baskette, VITA
VIII.	Conficker Brief	Bob Baskette, VITA
IX.	Upcoming Events	Peggy Ward, VITA

SARA

System Access Request Application

James Austin
Deputy Information Security Officer
VDOT Information Technology Division

VDOT APPLICATION ENVIRONMENT

- 9,000+ Users
- 10,000+ network accounts
- 150+ Applications
- Complex mix of Platforms
- Geographically dispersed offices throughout VA
- System access requests have historically been made through a paper form requiring ‘wet’ signatures

WHAT IS SARA?

Replacement of existing paper-based System Access Request Form (ITD-35A).

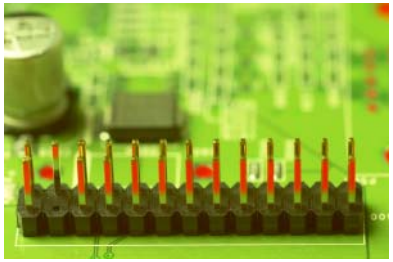
Centralized control point to Add, Change, or Delete user permissions.

Web-based application on VDOT's Intranet.

WHAT IS SARA?

Automated process flow with requests approved at several levels.

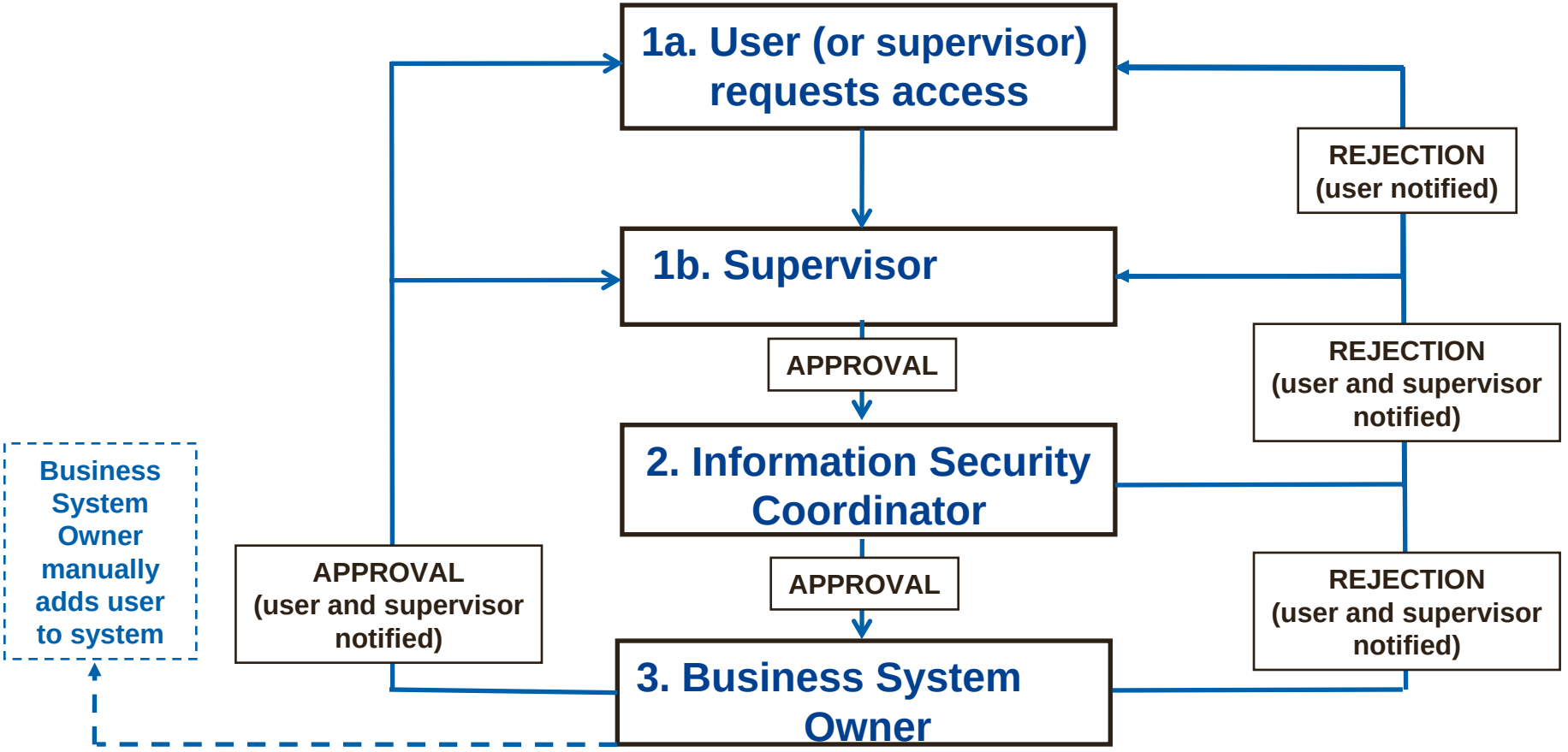
Chain of approval varies by system, work unit, and user role.



Does not interface automatically with other systems.

PROCESS

Uses VDOT's established approval levels:



NOTE: Additional levels can be added between existing ones.

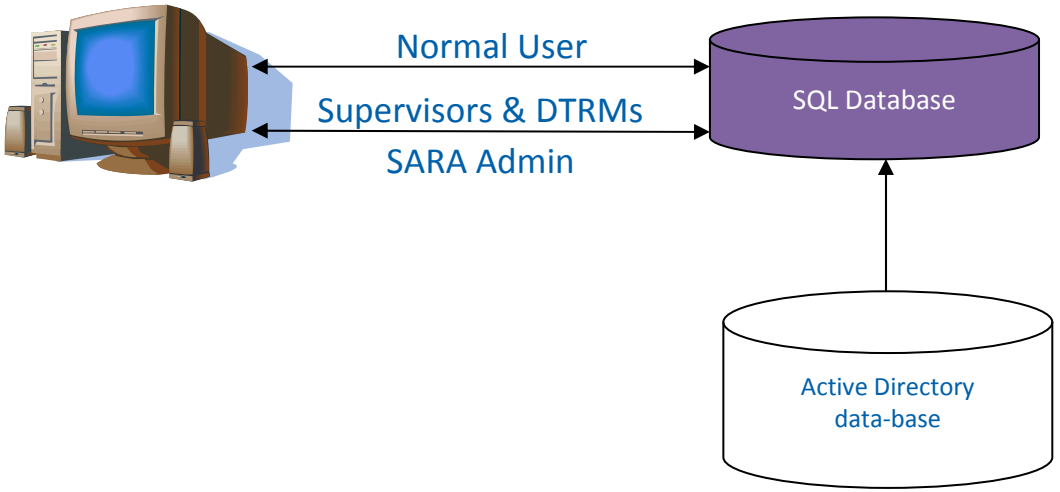
ARCHITECTURE

SARA consists of two main components:

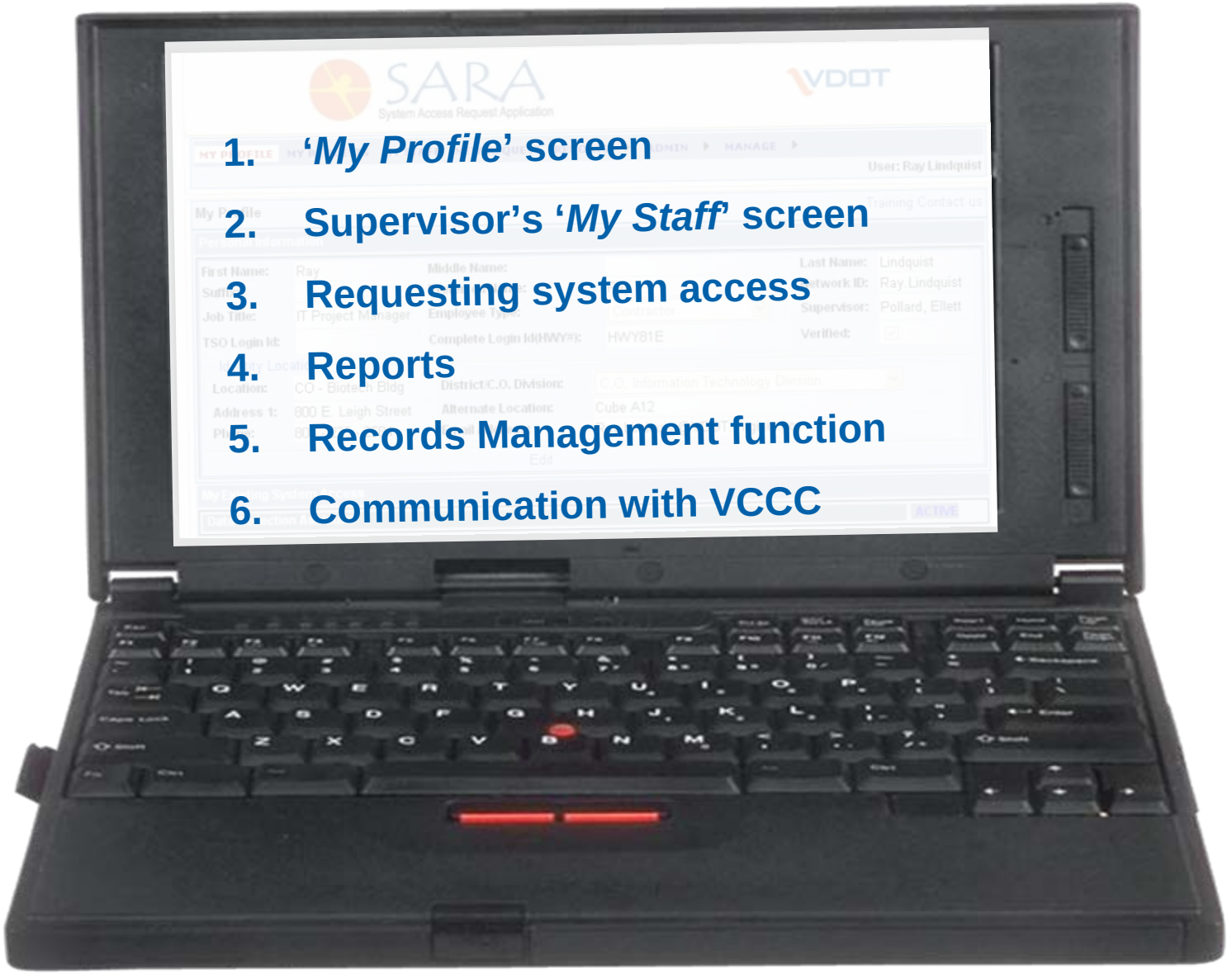
1. Presentation/Service layer

2. SQL Server Database layer

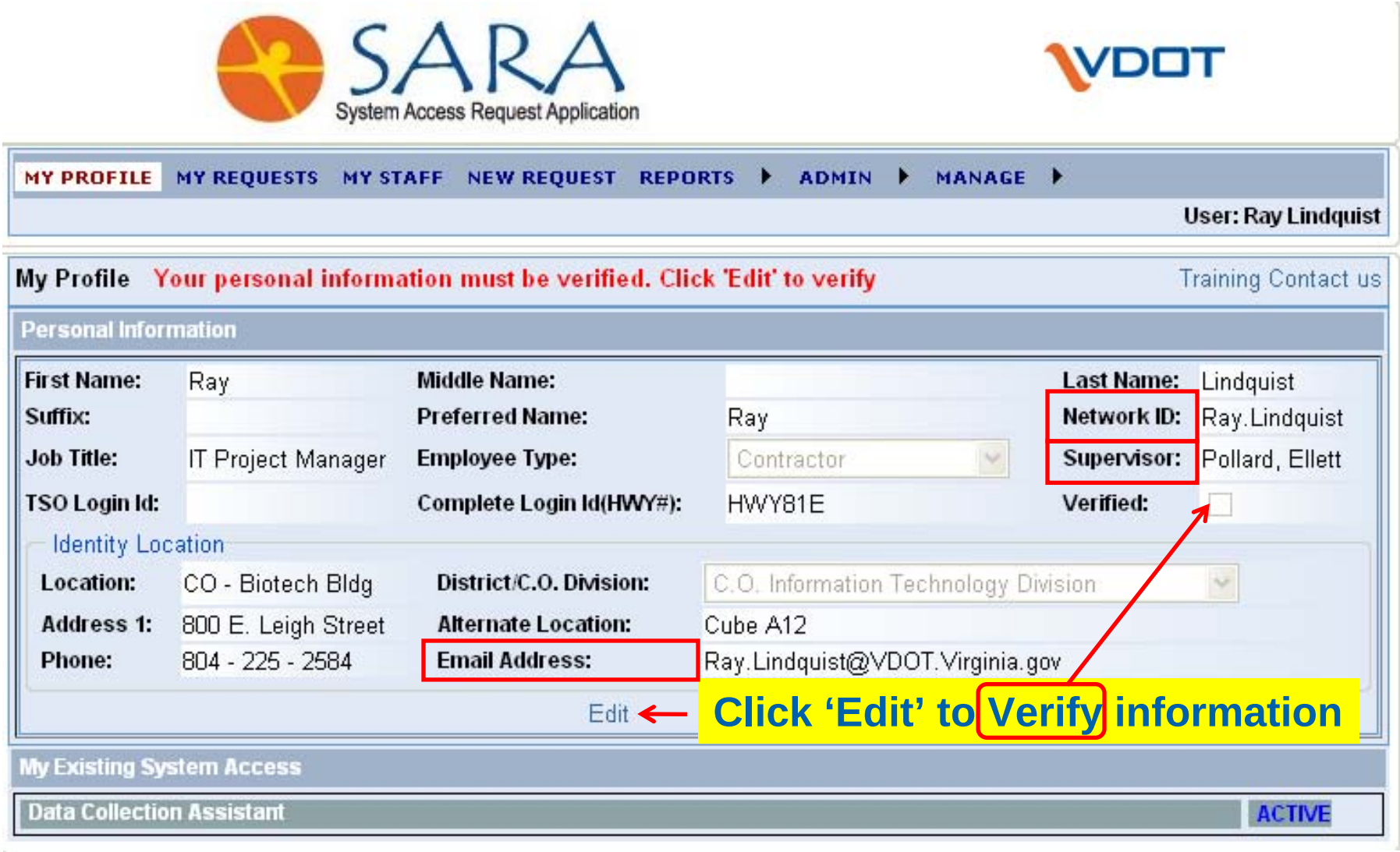
The Production environment receives nightly updates from Active Directory.



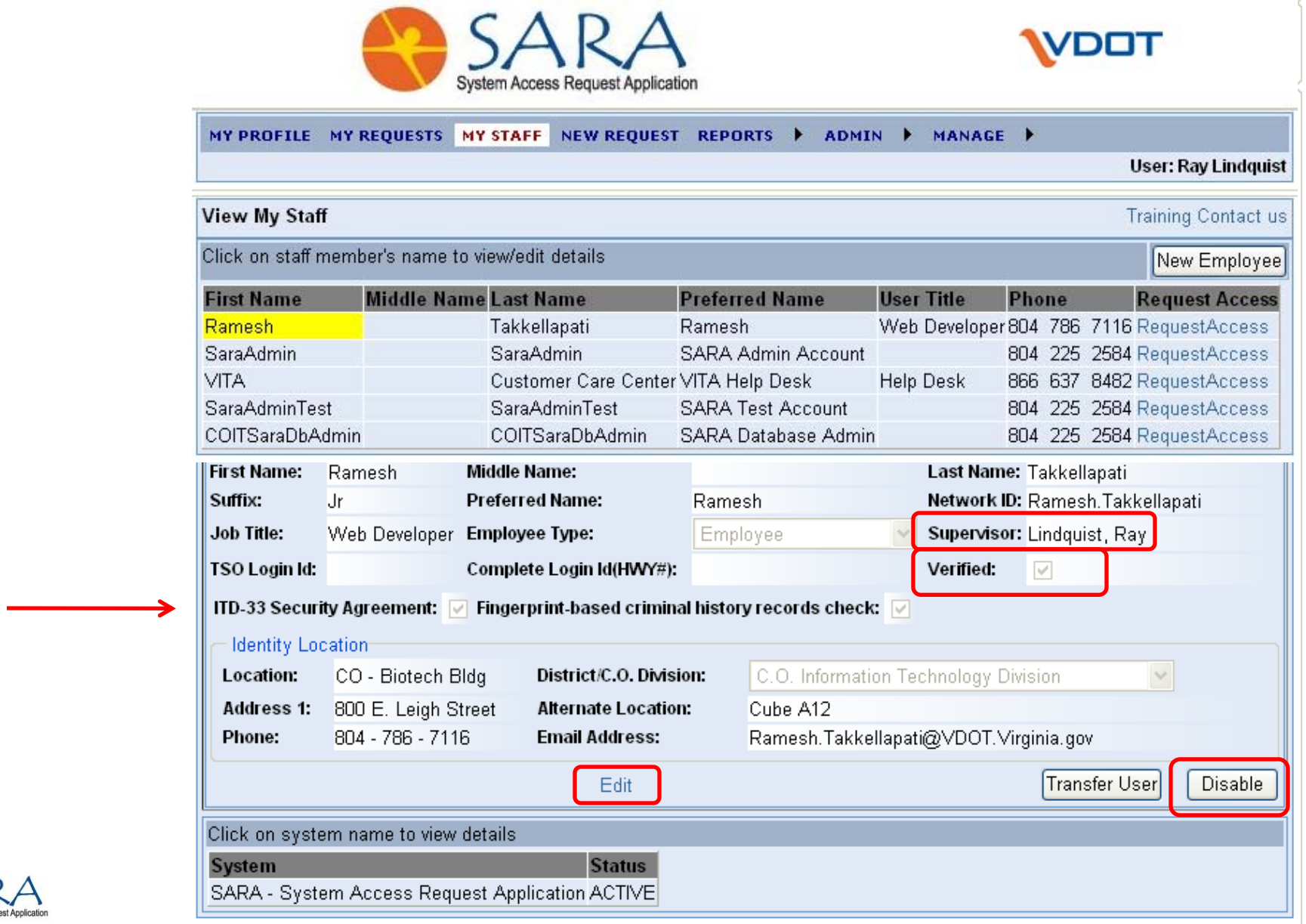
HOW DOES SARA WORK?

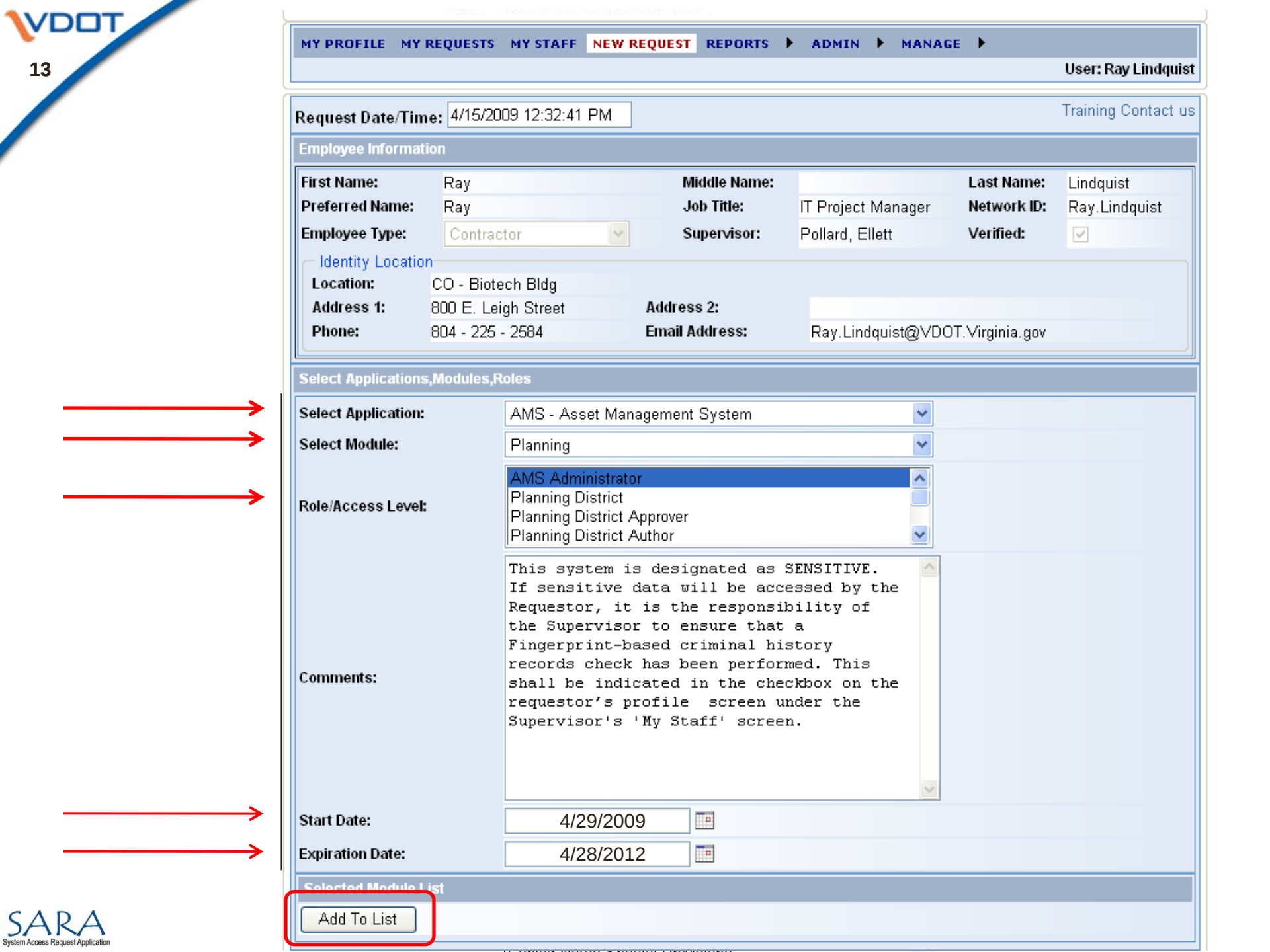


USER PROFILE



MY STAFF


SARA
System Access Request Application
VDOT
MY PROFILE
MY REQUESTS
MY STAFF
NEW REQUEST
REPORTS
ADMIN
MANAGE
User: Ray Lindquist
View My Staff
Training Contact us
Click on staff member's name to view/edit details
New Employee
First Name
Middle Name
Last Name
Preferred Name
User Title
Phone
Request Access
Ramesh
Takkellapati
Ramesh
Web Developer
804 786 7116
RequestAccess
SaraAdmin
SaraAdmin
SARA Admin Account
804 225 2584
RequestAccess
VITA
Customer Care Center
VITA Help Desk
Help Desk
866 637 8482
RequestAccess
SaraAdminTest
SaraAdminTest
SARA Test Account
804 225 2584
RequestAccess
COITSaraDbAdmin
COITSaraDbAdmin
SARA Database Admin
804 225 2584
RequestAccess
First Name: Ramesh
Middle Name:
Last Name: Takkellapati
Suffix: Jr
Preferred Name: Ramesh
Network ID: Ramesh.Takkellapati
Job Title: Web Developer
Employee Type: Employee
Supervisor: Lindquist, Ray
TSO Login Id:
Complete Login Id(HWY#):
Verified:
ITD-33 Security Agreement:
Fingerprint-based criminal history records check:
Identity Location
Location: CO - Biotech Bldg
District/C.O. Division: C.O. Information Technology Division
Address 1: 800 E. Leigh Street
Alternate Location: Cube A12
Phone: 804 - 786 - 7116
Email Address: Ramesh.Takkellapati@VDOT.Virginia.gov
Edit
Transfer User
Disable
Click on system name to view details
System
Status
SARA - System Access Request Application
ACTIVE



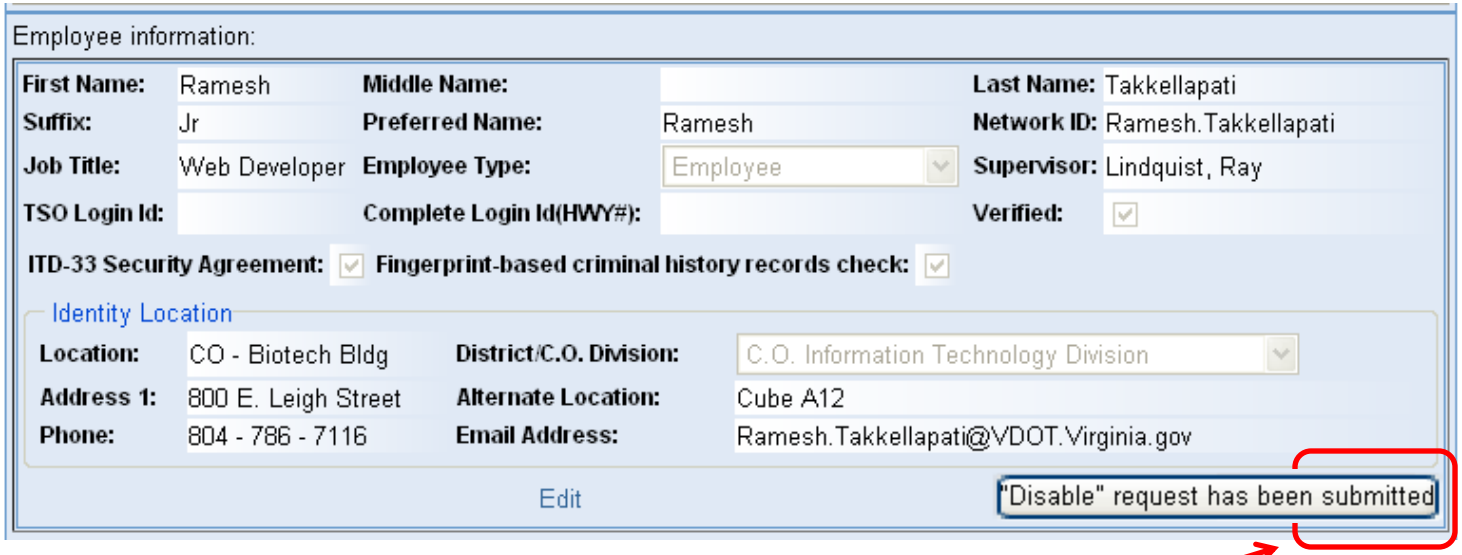
SARA
System Access Request Application

REPORTS

Reports available in Excel format

- **My Report**: Systems, modules, and access levels I have access to.
- **My Staff Report**: Same info for Supervisor's staff members.
- **DTRM Report**: Information on all staff in DTRMs respective district.
- **System Owner Report**: Lists staff with access to System Owner's system, modules, and at what levels.
- **Auditor's Report**: Same reports as DTRMs and System Owners as well as detailed Transaction History Reports.

RECORDS MANAGEMENT FUNCTION



1. Supervisor disables a staff member.
2. Email message is sent to all owners of systems to which this employee has access.
3. Requests cannot be made for this employee until the account is Enabled again.
4. After three years SARA sends VDOT Records Managers RM-3 form indicating that record(s) can be destroyed.

This screen mimics the form used by VITA/NG today

Select “Other Account” and additional data can be added

Automated communications between SARA and VCCC

Section 1: Employee or Contractor Information

Date: | Request Type: ☐ New ☐ Update ☐ Disable

Last Name: | First Name: | Middle Name:

Effective Date: | Agency Name: VDOT

Location: | District/C.O. Division: <--select-->

Work Address: | City: | Zip:

Employment Type:(select one)

☐ Classified employee — Employee ID:

☐ Wage employee

☐ Contractor — Expiration Date: — Contractor Company:

☐ Volunteer

Section 2: Account Requirements

☐ COV User account ☑ Other Account

For Contact requests only — E-mail Address for contact:

For Exchange resource account requests only — Type:
☐ Shared Calendar
(Calendar name)
(Calendar Manager)
☐ Conference Room
(Room name)
(Room Manager)

For Security group requests only — Name of group: / Group Manager:

For Service account requests only — Name of account:

For Test Account requests only — Name of account:

☐ Exchange mailbox(e-mail account) — Mailbox size: <--select>

☐ BlackBerry Service ☐ VPN Service

Business justification (required for account requests only):

Section 3: Additional Instructions/comments

Which security group(s) does the user need access to?

SARA System Access Request Application

BENEFITS

Comprehensive source of user and account information to improve management of system access.

Allows near real-time tracking of individual's permissions.

Managers use SARA to discontinue all application permissions with one click when users leave VDOT.

SARA speeds the process of obtaining system access.

- Electronic workflow
- Email notifications
- Backup approvers & reminders

SARA and AD RELATIONSHIP

SARA imports five data elements from Active Directory.

- User's Name, Network ID, Email Address, SID, and Status

Some Active Directory data out-of-date or inaccurate.

- Location, Title, Department, Office

The above data is kept current in SARA by VDOT users.

SARA does not update Active Directory.

NEXT STEPS

Information Technology Vision

Automated authentication that accounts have been disabled with automatic display of separation checklist.

SARA authenticates application access to systems.

Potential interfaces to inventory databases of:

- Production systems
- Software licenses
- Computer hardware
- MOAT training certifications

QUESTIONS?

Contact: **Jim Austin**, VDOT Deputy ISO
(804) 786-9315 or James.Austin@VDOT.Virginia.gov

Email Security

Messaging Encryption

Don Drew

IT Infrastructure Partnership Team

IT INFRASTRUCTURE PARTNERSHIP

VITA

NORTHROP GRUMMAN

Messaging Encryption

Agency Messaging Encryption Overview	As part of the effort to increase the security of the Commonwealth of Virginia (COV) IT Infrastructure, the Virginia Information Technologies Agency (VITA) will provide email encryption service after Messaging and Directory Services transformation has occurred at an Agency. This overview documents the steps required to obtain and use messaging encryption and the scenarios in which it may be used. The overview is intended as a reference document for use by Agency IT management.

Messaging Encryption

Process for Requesting Encryption Keys	1. Complete the **VITA/IT Infrastructure Partnership E-mail Mailbox and Account Request Form** and submit to the VCCC – Complete Section 7 – Required for Encrypted e-mail requests only – ISO approval and electronic signature is required – Users must already have been migrated to the COV domain for encryption 2. Once submitted to the VCCC, staff reviews the completed form for accuracy and appropriate approvals. Approved requests are forwarded to Messaging and Directory Services (MDS) Core Services for processing. 3. Once a request is approved and processed, the user is able to download and install the required certificates to enable encrypted email transmissions.

Messaging Encryption

User Instructions – 2 Reference Guides

How to Install a Certificate for Encrypted Email

1. Install the Certificate
2. View the Certificate
3. Manage the Certificate

How to Configure an Installed Certificate for Encrypted Email

1. Configure the Outlook Client
2. Configure Outlook Web Access

Digital Certificates

- To implement public key encryption on a large scale, digital certificates are used.
- COV users obtain certificates internally.
- Non-COV users obtain certificates from organizations such as VeriSign and TRUSTe.

Three Scenarios

1. *Internal to External*: An Internal COV User sends a message to an External Non-COV User.

   (a VDH user sends a message to Dr. Grey)

2. *External to Internal*: An External Non-COV User sends a message to an Internal COV User.

   (Dr. Grey sends a message to a VDH user)

3. *Internal to Internal*: An Internal COV User sends a message to another Internal COV User.

   (Department of Corrections user sends a message to a Virginia State Police user)

Virginia Information Technologies Agency

Policy, Standards and Guidelines Processes

John Green
Deputy Chief Information Security Officer

Policy, Standards & Guidelines Update

1. Collect comments & questions from the Information Security (IS) community during the year
2. Draft revision, or new policy, standard or guideline (PSG) addressing comments, and with input from staff & Information Security Officers (ISO)
3. Distribute draft to IS Council for review, input & feedback
4. Collect comments from IS Council, usually giving them a week or so to review
5. These comments are reviewed with Commonwealth Security & Risk Management (CSRM) Division management & addressed as appropriate in the PSG
6. Draft of PSG is sent to Information Technology Investment & Enterprise Solutions (ITIES) Directorate for review & comment
7. Aggregate comments from ITIES, usually takes a week or so
8. Comments from ITIES are reviewed with CSRM management & addressed as appropriate
9. Draft of PSG is sent to ITIES for posting to Online Review Comment Application (ORCA) for IS community review & comments
10. Gather comments from IS community (ORCA) for at least 30 days
11. Comments from IS community (ORCA) are reviewed with CSRM management & addressed as appropriate
12. Create responses to comments from ORCA reviewers & distribute them through ITIES
13. Finalized version of PSG is sent to ITIES who sends it to the CIO for approval.
14. If the CIO approves it goes to the ITIB for consideration & approval. If a standard or guideline there is a 5 day comment period & if a policy it must be approved at an ITIB meeting
15. Once approved it is posted to the web

Standard → 9

Policy → 10

Guidelines

IT Asset Mgmt, Facilities Security → 14

Virginia Information Technologies Agency

Payment Card Industry (PCI) Data Security Standards (DSS)

Peggy Ward
Chief Information Security & Internal Audit Officer

Are credit cards accepted by you or your service provider?

If YES – Your Agency/Locality Must Comply!

If YES – Your Agency/Locality Must Comply!

Any entity that accepts credit cards or has a service provider accept credit cards for them must comply or ensure their service provider complies with the PCI DSS in its entirety.
Here is an overview document
https://www.pcisecuritystandards.org/pdfs/pcissc_overview.pdf

You can download the Data Security Standard v 1.2 at
https://www.pcisecuritystandards.org/security_standards/pci_dss_download_agreement.html

Here is an overview of getting started:
https://www.pcisecuritystandards.org/pdfs/pcissc_getting_started_with_pcidss.pdf and a quick reference guide:
https://www.pcisecuritystandards.org/pdfs/pci_ssc_quick_guide.pdf

Here is an overview of the types of self assessment questionnaire necessary.
https://www.pcisecuritystandards.org/saq/instructions_dss.shtml#instructions

There are webinars available to help educate at
https://www.pcisecuritystandards.org/education/webinars.shtml

Virginia Information Technologies Agency

Administrative Measures - Security

Peggy Ward
Chief Information Security &
Internal Audit Officer

Administrative Measures

- Briefed at the 4/16 Agency Head Meeting
- Measured Annually
- Independent Source

Administrative Measures - Security

Information Technology			
Accessibility	Percent of compliance with IT accessibility standards *Source: DRS Accessibility Report*	90-100% 70-89% 0-69% Unavailable	
Information Security	Percent of compliance with information security standards *Source: VITA Information Security Report*	98-100% 95-97% 0-94% Unavailable	

Administrative Measures - Security

Source: Annual Report Information Security Report

1. Has an ISO been Designated?

2. Has a current Security Audit Plan been filed?

3. Are the Corrective Action due on file?

4. Are the Quarterly Updates due on file?

NOTE: IS Orientation attendance is not used as it is not a mandate!

§ 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	CAP's Received	Quarterly Updates
Agency XYZ	YES	10	Yes	Yes	Yes

Acronyms:
ISO – Information Security Officer
IS – Information Security
CAP – Corrective Action Plan

ISO Designated
Yes - The agency head has designated an ISO for the agency within the past two years.
No - The agency head has NOT designated an ISO for the agency within the past two years.

Attended IS Orientation
The number indicates how many agency personnel have attended the optional Information Security Orientation sessions indicating they are taking additional, voluntary action to improve security at their agency akin to "Extra Credit!"

Security Audit Plan Received
Yes - The agency head has submitted a Security Audit Plan for systems classified as sensitive based on confidentiality, integrity or availability.
No - The agency head has NOT had a Security Audit Plan submitted for systems classified as sensitive based on confidentiality, integrity or availability.
Exception – The agency head has submitted and the CISO has approved a temporary exception on file with VITA to allow time for developing the security audit plan.

Explanation – Continued

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAP's Received	Quarterly Updates
Agency XYZ	YES	10	YES	YES	YES

Corrective Action Plans Received & Quarterly Updates Received

Yes - The agency head has submitted an adequate Corrective Action Plan/Quarterly Update for Security Audits scheduled to have been completed.

Some - The agency head has submitted an adequate Corrective Action Plan/Quarterly Update for some but NOT all Security Audits scheduled to have been completed.

No - The agency head has NOT submitted an adequate Corrective Action Plan/Quarterly Update for Security Audits scheduled to have been completed.

Not Due - The agency head did not have Security Audits scheduled to be completed or has submitted a corrective action plan within the last quarter and no quarterly update is due.

N/A - Not applicable as the agency head has not submitted an Information Security Audit Plan or a Corrective Action Plan that was due.

Secretariat: Administration

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAP's Received	Quarterly Updates
Human ~~Resource~~ Rights Council	YES	0	NO	N/A	N/A
Dept. of General Services	YES	0	YES	NO	N/A
Dept. of Human Res. Mgmt	YES	0	YES	Not Due	Not Due
Dept. Min. Bus. Enterprise	YES	2	NO	N/A	N/A
Employee Dispute Resolution	YES	3	YES	Not Due	Not Due
Compensation Board	~~NO~~ YES	1	YES	NO	N/A
State Board of Elections	NO	0	YES	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	YES	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	~~NO~~ YES	~~N/A~~ Not Due	~~N/A~~ Not Due
Board of Accountancy	YES	1	YES	NO	N/A
Dept. of Housing & Community Development	YES	1	YES	Some	Not Due
Dept. of Mines, Minerals & Energy	YES	1	YES	Some	NO
Dept. of Labor & Industry	YES	3	NO	N/A	N/A
Dept. of Professional & Occupational Regulation	YES	1	YES	NO	N/A
Tobacco Indemnification Commission	YES	0	NO	N/A	N/A
Va. Employment Commission	YES	3	YES	NO	N/A
Va. Economic Development Partnership	YES	0	NO	N/A	N/A
Va. Housing Development Authority	NO	1	NO	N/A	N/A
Va. National Defense Industrial Authority	NO	0	NO	N/A	N/A
Va. Resources Authority	NO	0	NO	N/A	N/A
Va. Racing Commission	YES	2	YES	Not Due	Not Due

Secretariat: Education

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAP's Received	Quarterly Updates
Dept. of Education	YES	1	YES	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	0	YES	NO	N/A
Library of Va.	YES	1	YES	Not Due	Not Due
State Council of Higher Education for Va.	YES	0	NO	N/A	N/A
Science Museum of Va.	YES	0	NO	N/A	N/A
Va. Commission for the Arts	YES	0	NO	N/A	N/A
Va. Museum of Fine Arts	YES	2	YES	YES	Not Due

Secretariat: Education (Cont'd)

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAP's Received	Quarterly Updates
Christopher Newport University	YES	0	YES	Not Due	Not Due
George Mason University	YES	1	YES	Some	YES
James Madison University	YES	0	YES	YES	Some
Longwood University	YES	1	YES	YES	YES
Norfolk State University	YES	2	NO	N/A	N/A
Old Dominion University	YES	1	YES	YES	YES
Radford University	YES	0	YES	YES	YES
University of Mary Washington	YES	1	YES	NO	N/A
Va. Community College System	YES	36	YES	Some	~~NO~~ YES
Virginia Military Institute	YES	0	YES	NO	N/A
Virginia State University	YES	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	NO	N/A	N/A
Dept. of Planning & Budget	YES	2	~~NO~~ YES	~~N/A~~ Not Due	~~N/A~~ Not Due
Dept. of Taxation	YES	1	YES	Some	YES
Dept. of Treasury	YES	2	YES	~~NO~~ YES	~~N/A~~ Not Due

Secretariat: Health & Human Resources

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAP's Received	Quarterly Updates
Dept. of Health Professions	YES	0	YES	Not Due	Not Due
Dept. of Medical Assistance Services	YES	6	YES	Some	Not Due
Dept. of Mental Health, Mental Retardation, & Substance Abuse Services	YES	15	YES	Not Due	Not Due
Dept. of Rehabilitative Services	YES	0	YES	NO	N/A
Dept. of Social Services	YES	2	YES	NO	N/A
Tobacco Settlement Foundation	NO	0	NO	N/A	N/A
Va. Dept. for the Aging	YES	1	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	1	YES	Some	Not Due
Dept. of Environmental Quality	YES	4	YES	YES	Some
Dept of Game & Inland Fisheries	YES	1	NO	N/A	N/A
Dept. of Historic Resources	YES	2	YES	Not Due	Not Due
Marine Resources Commission	YES	1	YES	YES	~~YES~~ Not Due
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	1	YES	YES	Some
Commonwealth's Attorney's Services Council	NO	0	NO	N/A	N/A
Dept. of Criminal Justice Services	YES	2	YES	NO	N/A
Dept. of Fire Programs	YES	3	YES	Not Due	Not Due
Dept. of Forensic Science	YES	1	YES	Not Due	Not Due
Dept. of Juvenile Justice	YES	3	YES	NO	N/A
Dept. of Military Affairs	NO	1	NO	N/A	N/A
Dept. of Corrections	YES	3	YES	Some	Not Due
Dept. of Correctional Education	YES	1	NO	N/A	N/A
Dept. of Veterans Services	YES	1	NO	N/A	N/A
Va. Dept. of Emergency Management	YES	1	NO	N/A	N/A
Va. State Police	YES	3	YES	Not Due	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	YES	NO	N/A
Va. Info. Technologies Agency	YES	33	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	2	NO	N/A	N/A
Dept. of Rail & Public Trans.	YES	1	YES	Not Due	Not Due
Motor Vehicle Dealers Board	YES	0	NO	N/A	N/A
Va. Dept. Of Transportation	YES	5	YES	YES	Some

Independent Branch Agencies

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAP's Received	Quarterly Updates
Indigent Defense Council	YES	4	~~NO~~ YES	~~N/A~~ Not Due	~~N/A~~ Not Due
State Lottery Dept.	YES	2	NO	N/A	N/A
State Corporation Commission	YES	3	YES	Not Due	Not Due
Va. College Savings Plan	YES	3	YES	Not Due	Not Due
Va. Office for Protection & Advocacy	YES	1	EXCEPTION	EXCEPTION	N/A
Va. Retirement System	YES	2	YES	Not Due	Not Due
Va. Workers' Compensation Commission	YES	1	EXCEPTION	EXCEPTION	N/A

Others

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAP's Received	Quarterly Updates
Office of the Governor	YES	3	EXCEPTION	EXCEPTION	N/A
Office of the Attorney General	YES	1	YES	Not Due	Not Due

Totals

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAP's Received	Quarterly Updates
Totals:	Y- 81 (92%) N- 7 (8%) ~~Y- 80 (91%)~~ ~~N- 8 (9%)~~	231 from 65 (74%) of 88 agencies	Y-59 (67%) N – 26 (30%) Exceptions – 3 (3%) ~~Y- 56 (64%)~~ ~~N- 29 (33%)~~	Y-12 (14%) Some – 8 (9%) N – 15 (17%) Not Due – 24 (27%) N/A – 26 (30%) Exceptions – 3 (3%) ~~Y- 11 (13%)~~ ~~N- 16 (18%)~~ ~~Not Due- 21 (24%)~~ ~~N/A- 29 (33%)~~	Y-8 (9%) Some – 4 (5%) N – 1 (1%) Not Due – 31 (35%) N/A – 44 (50%) ~~N- 2 (2%)~~ ~~Not Due- 26 (30%)~~ ~~N/A- 48 (54%)~~

Virginia Information Technologies Agency

Latte Larceny

Bob Baskette, CISSP, CCNP
Incident Management Engineer

Why Information Security Matters

The need for Information Security

- Computer systems have an inherent value to both the computer system owner and those malicious individuals who seek the data stored on the computer systems and the available processing power the computer systems possess.
- Malicious individuals may also be interested in taking over the computer system to store illegal materials or launch attacks that will be traced back to the compromised system instead of the malicious individual.

Open Access Environments

- Open Access Environments come in two basic forms
  - Truly open access
    - Anyone can connect
    - No password required
    - No time limit
  - Pay for Play
    - Need to purchase access time or a store item
    - Will require a passphrase or access code
    - May have a time limit or one-time use limit

- Open Access environments simply provide access to the Internet. They do not provide or are responsible for system security = Caveat emptor

- Types of Open Access environments
  - Coffee shops
  - Airports
  - Bookstores
  - Car Dealers
  - Restaurants
  - Libraries

Physical Threats in an Open Access Environment

- Theft
  - Computer Equipment and components
  - Paperwork/Files/Print-outs
- Shoulder surfing
  - Camera phones
  - Parking lot cameras/camcorders
  - People waiting in line (Old School)
  - Cell phone conversations

Hybrid Threats in an Open Access Environment

- Removable Media
  - USB Flash Drives
  - CD/DVD
  - iPod/MP3 players

- Social Engineering
  - Friendly people want to share
    - “Funny” email
    - “Cool” song
    - “Amazing” videos

Electronic Threats in an Open Access Environment

- Rogue Access Point
  - Provide Man-In-The-Middle attack platform
  - Spoofs a legitimate AP
  - Wireless client sends all traffic to rogue AP
  - Rogue AP copies all interesting traffic prior to sending to the legitimate destination

- Wireless sniffers/snoopers
  - Captures all traffic sent within a specific spectrum
  - Can store and extract information within the wireless network packets
  - Storage capacity only limited by available hard drive space
  - Can be tuned to monitor a specific computer or every computer in reception range
  - Wireless sniffing software can be downloaded from the Internet for free and runs under all major operating systems

Electronic Threats in an Open Access Environment

- Ad-hoc access
  - Most operating systems support the concept of peer-to-peer/laptop-to-laptop/Ad-Hoc connections
  - Two laptops can communicate directly without the need for a wireless access point
  - Equivalent to allowing a malicious individual to connect an Ethernet cable to the laptop
  - Some operating systems support the concept of a wireless bridge which allows an Ad-hoc connected computer to use the Infrastructure connection to reach other networks. The malicious individual could use the Ad-Hoc connection to reach a private LAN

Defense In Depth – Be Aware

Just because you are paranoid, that does not mean that someone is not out to get you

- Do not leave the computer unattended
  - Laptops and components can grow legs when not watched
  - USB and Firewire ports are exposed to walk-by insertion/infection
- Be aware of your surroundings
  - Be wary of people just “hanging around”
  - Be cautious of window seats and large mirrors
- Be cautious of “Helpful” people
  - Be wary of non-employees who want to help with the wireless connection
  - Avoid people who offer free connections at a “Hot-Spot” that normally charges for a connection

Defense in Depth – The Geek Speak

- Operating System Hardening
- Anti-X software
- Email Best Practices
- Secure Internet usage
- Software firewall with SPI functionality
- Enable encrypted VPN session
- Avoid Split-Tunneling
- Avoid Ad-Hoc wireless configuration
- Turn off the wireless radio when not in use

Operating System Hardening

- Every modern Operating System has vulnerabilities and available exploits with which to attack those vulnerabilities.
- To protect the Operating System:
  - Enable the “Automatic Software Update” feature.
  - Disable the “Auto-Run” feature.
  - Remove software that is no longer needed.
  - Remove trial software once the trial has ended.
  - Do not install unsolicited software from any source.
  - Turn off File Sharing, Print Sharing, NetBios or other services that are not needed.

Operating System Hardening

- Employ the Least Privilege concept
  - Create a separate account for system administration on the computer system.
  - Do not use the name Admin, Superuser, Root, or any other term that would suggest that the account is the Administrator account. The “Administrative” account should only be used to install software and make system modifications.

- Create separate accounts for each user on the computer system. The user accounts should be used for the day to day activities. Limiting access to the system privileges associated with the Administrator account will prevent some of the malicious content spreading across the Internet from getting installed on the computer system.

Operating System – Password Selection

- Ensure that each account on the computer system uses strong passwords.
  - Do not use anything that can be associated with the user such as name, birth date, family member/pet name, or words found in the dictionary.
  - A password should not relate to the image used by the screensaver.
  - Use phrases or build a password by pulling out the first and last letter of every word of a phrase and use that as the password.
  - Replace characters with numbers such as the ‘0’ (zero) instead of the ‘O’, ‘1’ instead of an ‘i’, ‘3’ instead of an ‘e’, or ‘4’ instead of an ‘a’.

Anti-X software

- Every computer system needs an up-to-date version of anti-virus, anti-spyware, anti-spam, and anti-phishing software.
- Configure the Anti-X software to check for product updates on a daily basis.
- Configure the Anti-X software to scan the entire contents of the hard drive at least once a week.
- Configure the Anti-X software to scan ALL removable media each time the removable media is attached to the computer system.
- Scan ALL installation CD/DVDs for malicious code prior to installing the software.
- Do not let the Anti-X software expire. Please renew the software update license each year or purchase a new copy of the software at the end of each year.

Anti-X Notes

- Before any USB device is used:
  - Turn off the Operating System “Auto-Run” feature.
  - Scan the device for malicious software.
- Monitor the computer system:
  - Monitor hard disk space to determine if the available space decreases for an unknown reason – This may indicated a backdoor has been installed on the computer system and the system is storing information for a malicious individual.
  - Monitor the log files and Event Viewer logs for unexpected error messages.
- Avoid P2P programs. Multimedia download services such as Limewire, Bearshare, Gnutella and Kazaa can expose the computer system to massive exploits.

Email Security Best Practices

- To mitigate the potential threat presented by a spam or phishing email campaign, never open attachments or click links contained in unsolicited email messages.
- If possible, check with the person who supposedly sent the email to make sure that it is legitimate prior to opening any attachments.
- Scan any attachments with anti-virus software before opening the attachment.
- Do not reveal personal or financial information in an email, and not to respond to email solicitations for this information.

Email Security – Additional Steps

- Always examine the URL of a web site. Malicious web sites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain extension such as .com vs. .net.
- If the legitimacy of an email request needs to be verified, try to verify the origin of the email by contacting the company directly. Never use the contact information provided on a web site connected directly to the email request.
- An additional step to help mitigate the risk of a phishing campaign is to limit the administrative rights of the local users through the implementation of the Least-Privileged best practice.
- Disable automatic image loading.

Secure Internet Usage

- Modern-day Browsers
  - Microsoft Internet Explorer 7
  - Mozilla Firefox 3
  - Safari 3
- Browser configuration
  - Disable Active-X controls and applets if possible.
  - Disable the Adobe Flash plug-in if possible.
  - Disable form auto-fill functions.
  - Disable password caching.
  - Install security plug-ins from the software vendor's website to improve the security inspection of the displayed website.
  - Configure the browser to clear all browser information when the browser window is closed.
  - Only accept cookies from the sites that you visit.

Additional Secure Internet Usage

- Avoid Tab browsing when sending sensitive information.
- Prior to initiating a secure connection to a website where confidential information will be sent to or received from the web server:
  - Close all browser windows.
  - Clear the browser cache.
  - Clear all browser cookies.
- Enable private browsing if supported by your browser.
- Do not ignore SSL certificate warnings.
- Beware of the “Pop-Up” window. Never install a program just because a “Pop-Up” window appears with message indicating that a software update or applet is needed. Remember, if a trusted website prompts to install a program, err on the side of caution and say no. Contact the company by telephone and confirm the software update.

Secure Internet Usage Password Security

- Use strong passwords for any websites requiring a login.
- Use unique passwords for all websites. Avoid using the same password for similar websites.
- Carefully consider the questions used by a website for automated password resets. Most websites use the same set of common questions for password reset. Most of the answers to these questions can be found in public records or on-line.
  - Place of birth, mother's maiden name, and school information are available in public records.
  - Friends, color preference, hobbies, and pet information often found on Social Network sites.
  - Make of first car can be guessed based on purchasing trends.
  - Consider using the option to create your own question/answer combination if possible.

Software Firewall Configuration

- A software-based firewall with Stateful Packet Inspection technology should be installed on any mobile computing device. SPI technology will examine traffic destined for the mobile computing device to determine if the inbound traffic is arriving in response to an authorized request.

- Implement a “Client-Only” or “Established/Related” traffic filtering list.
    - Allow only the inbound network traffic that is needed.
    - Define the programs, protocols and ports that should have access to the home network.
    - Block unsolicited traffic from connecting to the home network.
    - Prevent LAN traffic from leaving the home network .
    - Filter all inbound traffic with a source IP-address in the RFC-1918 Private IP-address range.
    - Filter all inbound traffic with a source IP-address that matches the IP-address range used on the home network.

- Enable the “automatic update” feature if one exists for the firewall.

- Periodically check the firewall vendor’s website for the latest software updates.

- Firewalls should be configured to log activity. These logs should be reviewed at least once a month to identify any anomalous or unexpected activity.

VPN concepts

- Enable encrypted VPN session
  - Provides data protection regardless of the wireless network configuration
- Avoid Split-Tunnel VPN configurations
  - Split-Tunnel VPN configurations allow traffic to either transverse the VPN tunnel or the Internet.
  - Split-Tunnel VPN configurations expose the VPN network to threats that exist in the Internet
- Avoid Ad-Hoc connections
  - Configure the computer system to operate in an “Infrastructure Mode” only.
    - Wireless “Ad-Hoc” mode will allow a direct connection between two computers using wireless network adapters.
    - Microsoft Windows 2000/XP will bridge an active wireless connection to the wired network in certain network configurations.
    - An “Ad-Hoc” connection to a computer system may allow a malicious individual to “by-pass” all security measures and connect to the remote VPN network.

Choose Security

- Ask about available Wi-Fi security
- Most Open Access environments provide little security protection mechanisms, but it never hurts to ask.
- Enable Wi-Fi Protection
  - WPA-2 Personal security provides the best protection.
  - WPA security provides adequate protection.
  - WEP has been compromised, but is still better than clear text.

Helpful URLs

- To learn more about network security, please visit the following sites:
  - http://www.securityfocus.com/columnists/385
  - http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf
  - http://www.isc.sans.org
  - http://www.microsoft.com/protect/default.mspx
  - http://www.microsoft.com/security/default.mspx
  - http://www.us-cert.gov
  - http://www.us-cert.gov/cas/tips/ST04-004.html
  - http://onguardonline.gov/tutorials/firewall-xp-instruct.html
  - http://onguardonline.gov/tutorials/firewall-osx-instruct.html

Final Thoughts

- The security of a computer system is ultimately decided by how the computer system is used.
- A “Fully-Patched” computer system is only fortified against known vulnerabilities. “Zero-Day” exploits and unpublished vulnerabilities can still have a negative impact on the computer systems.
- Most computer systems that become compromised have two components in common.
  - The computer system had outdated anti-virus programs
  - The computer systems were used to download music and movies from the Internet.
- Keep the software on the computer systems up-to-date.
  - Install the latest security updates from the software vendor.
  - Enable Automatic Updates for the operating system, anti-virus, and user applications.

Final Thoughts

- Scan the computer system for malicious software at least once a week.
- Back-up your files on a regular basis.
- Keep all installation CD/DVD media and license keys in a safe place.
- Visit computer security websites to become aware of the current malicious threats.
  - www.isc.sans.org
  - www.us-cert.gov
  - www.securityfocus.com

Questions???

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

Thank You!

Virginia Information Technologies Agency

Variations on a Theme: Conficker worms and the need for Patch Management

Bob Baskette: CISSP, CCNP
Commonwealth Security Incident Management Engineer

What's in a Name

- The Conficker worm is also known as the Downadup worm, the Downup worm, and the Kido worm. There are five variants of the worm are known to exist in the wild.
- The Conficker worm can propagate through a previously patched stack buffer overflow vulnerability in Microsoft Windows Server Service (MS08-067) used by Windows 2000, Windows XP, Windows Vista, Windows Server 2003, Windows Server 2008, and Windows 7 Beta.
    - http://www.microsoft.com/technet/security/Bulletin/MS08-067.mspx)
- The Conficker worm propagates through the use of a Server Message Block (SMB) Session Setup Request to determine if the remote system is vulnerable to attack based on operating system and patch level. The worm is distributed as a dynamic linked library (DLL) and establishes a stealth service.
- The Conficker worm will copy itself to the file system using a random name and modifies registry keys under HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ .
- Once resident on a vulnerable computer, the Conficker worm disables a number of system services such as Microsoft Windows Automatic Update, Microsoft Windows Security Center, Microsoft Windows Defender, and Microsoft Windows Error Reporting.

Conficker Basics

- The Conficker worm can also propagate via infected removable media such as USB drives and CD/DVDs.
- The Conficker worm is most effective within computing environments that have open Microsoft Windows shares, weak passwords, a lack of current software updates, and unrestricted Autorun functionality for removable media.
- Symptoms of infection
  - Account lockout policies reset automatically without intervention
  - Microsoft Windows Domain controllers respond slowly to requests
  - Unusually high system network utilization
  - Security websites cannot be contacted
  - Port 445/TCP scanning with variant A/B/E
  - Multicast UPnP requests
  - High-range TCP-port and UDP P2P Activity
  - Abnormal DNS lookup activity
- The worm also attaches itself to certain Windows processes such as svchost.exe, explorer.exe and services.exe.
- Over 8500 computers known to be infected in Virginia with an estimated 3-Million infected worldwide.

Malicious Software Definitions

- Virus = A computer program that can generate multiple copies of itself as well as infect a computer system without the knowledge of the system owner.

- In order to replicate, a virus must execute malicious code. Much like in nature, a computer virus is inert and cannot perform its malicious mission until it is inserted into a host file (some type of executable code).

- A virus can only spread from one computer system to another computer system when its host file is first transferred to the target computer system. The most common methods for virus transmission are via a network connection or removable medium such as a CD/DVD or USB drive.

Virus Types Based on Behavior

- Viruses types based on execution behavior.
  - Nonresident viruses
    - Begin searching for target hosts to infect as soon as the virus is activated.
    - Once the target is infected, the virus will transfer control to the application program it infected.
  - Resident viruses
    - Resident virus loads itself into memory upon execution and transfers control to the host program.
    - The virus will stay active in memory and will infect new host files only when those files are accessed by other programs or the operating system itself.
  - Nonresident viruses have a finder module and a replication module
    - The finder module is responsible for finding new files to infect.
    - The replication module is responsible for actually infecting the file.
  - Resident viruses contain only a replication module
    - Resident viruses contain a replication module, but not a finder module since the replication module is executed each time the operating system is called to perform a certain operation.

Malicious Software Definitions

- Worm = A self-replicating computer program which will exploit security vulnerabilities to spread itself to other computer systems without the need to be transferred as part of a host file.
- A worm can utilize either a network connection or removable media to propagate to other computer systems.
- This propagation can occur as a system background task and usually does not require user interaction.
- Worms almost always cause some disruption to the network (normally consuming bandwidth) whereas a virus will corrupt or destroy files on a targeted computer system.
- Most worms will either carry a “Payload” or download the “Payload” once the worm has taken control of the computer system. A popular payload for a worm is a “Backdoor” program to allow the creation of a "zombie", which will be controlled by the worm author.

Malicious Software Definitions

- Trojan horse (AKA Trojan) = A computer program that appears to perform a desirable function but in fact performs a malicious function.

- Trojan programs allow unauthorized access to the host computer, providing the malicious individual the ability to save files on the compromised computer or capture data processed on the compromised computer.

- The six main types of Trojan horse payloads are:
  - Remote Access
  - Data Destruction
  - Downloader/dropper
  - Server Trojan (Proxy, FTP , IRC, Email, HTTP/HTTPS, etc.)
  - Disable security software
  - Denial-of-service attack (DoS)

Conficker A

- Conficker.A is a computer worm that appeared on November 21st, 2008 and targets the Microsoft Windows operating system.
- Conficker.A began infecting systems 29-days after Microsoft released the software update to resolve the issues associated with the vulnerability in the Microsoft Server Service.
- Conficker.A attempted to exploit the vulnerability by sending a specially crafted Remote Procedure Call (RPC) request over TCP-port 445.
- Conficker.A contained an instruction to prevent it from infecting systems containing the Ukrainian keyboard mappings.
- Conficker.A will generate a HTTP server and open a random port between 1024 and 10000. If the remote machine is exploited successfully, the victim will connect back to the HTTP server and download a worm copy. (with a .jpeg extension).
- It will also reset System Restore points, and download files to the target computer.

Conficker B/B++

- Conficker.B variant excludes the Ukrainian keyboard check contained in the Conficker.A variant.
- Conficker.B disables installed system-level anti-virus products and utilizes scheduled tasks for re-infection.
- Conficker.B has been modified to infect patched systems via removable media (USB drives) and brute-force password-guessing.
- Conficker.B will also generate a HTTP server and open a random port between 1024 and 10000. If the remote machine is exploited successfully, the victim will connect back to the HTTP server and download a worm copy (with a .jpg extension). It will also reset System Restore points, and download files to the target computer.
- Conficker.B++ variant implements a new backdoor with “auto-update” functionality which will allow compromised systems to have additional malicious binaries installed on them from remote systems without relying on the previous variants’ command and control (C2) network.
- This backdoor feature is an attempt by the operators of the Conficker network to evade the detection and blocking techniques developed in response to the Conficker.A and Conficker.B behavioral patterns.

Conficker C/D

- Conficker.C utilizes a P2P communication system involving both TCP and UDP for propagation.
- Conficker.C also employs multiple security countermeasures to defeat detection and removal procedures.
  - Conficker.C alters the DNS resolution services of the infected computer systems to prevent domain name lookups for a variety of security services and vendor sites.
  - Conficker.C disables the local anti-virus update services.
  - Conficker.C disables the Windows Firewall from blocking several high TCP and UDP port numbers in order to ensure its P2P communications capability.

Conficker C/D Additional Information

- The total number of top level domains (TLD) used by the domain name generation algorithm has been increased to 116 and the list of domain names generated is now 50,000 per 24 hours, 500 of which are then randomly selected and queried.
- Instead of using a list of known peers, Conficker.C scans remote addresses in a semi-random fashion for listening peers. Once an infected peer is located and the P2P network is joined, file transfer is possible, including the uploading or downloading of signed binary updates.
- The ".D" variant tag was inappropriately assigned to a sub-type of the ".C" variant, therefore the ".D" variant tag will not be used for any future variants of the worm to avoid confusion with the ".C" sub-type.

Conficker E

- Conficker.E is the latest variant of the Conficker Worm.
- Conficker.E began spreading on April 9, 2009. This variant appeared 168-days after Microsoft released a software updated to resolve the vulnerability associated with MS08-067.
- Conficker.E updates earlier infections via its peer to peer (P2P) network as well as resuming scan-and-infect activity against unpatched systems that was utilized by the ".A", ".B", and ".B++" variants.
- Conficker.E is also capable of installing and operating a web serve that utilizes TCP-port 5114.
- The primary function of Conficker.E is to serve as a "BOT" framework for other malicious software.
- Conficker.E attempts to download additional malicious code onto victim systems, including copies of the Waledac Trojan(a spam-oriented malicious application which has previously propagated only via bogus email messages containing malicious links).

What so special about Conficker

- Framework for malicious activity
  - Phishing
  - Spam
  - Key-Logging software
  - Ransomware / ScareWare
- Can be spread via network activity or via USB devices with embedded malware
- Has evolved through five variants in less than 170-days.
- The worm is using modern encryption and Hashing technologies and is applying software updates to those technologies as required to eliminate vulnerabilities.

Waledac Malicious Software

- The Waledac family of malicious has been closely associated with Conficker.
- Waledac has access to over 200 domains to store and distribute malicious software.
- Waledac was used to distribute SpywareProtect2009 on April 8, 2009.
- The Waledac family of malicious software contains spam engines, key-loggers, and RansomWare/ScareWare
- The Waledac authors prey on fear and mistrust to spread malicious softwareand has used themes about the Economic Crisis and personal turmoil as social engineering lures.
    - Recent E-mail Spam Subject Lines:
        - Are you sure in your partner's faithfulness?
        - Does your partner truly love you?
        - Do you know whom is she sending sms? Do you really trust her?
        - Do you trust your partner blindly?
        - Suspect your partner is being unfaithful?
- Waledac spam engines are used for both traditional unwanted advertisements for pharmaceuticals, pornography, or other cheap products as well as “Joe Jobbing” commercial websites.

Waledac Spam terms and objectives

- Joe Job = A spam attack using spoofed sender data that is intended to tarnishing the reputation of the spoofed sender and/or induce the recipients of the spoofed email to take action against the spoofed sender. The spam attack will simply advertise the victim's product, business or website or it may also claim that the spoofed sender is selling illegal or offensive items such as illegal drugs, automatic weapons or child pornography to increase the likelihood that the recipient will take action against the victim. The spam attack can also lead to a temporary Denial-of-Service condition for the spoofed sender's website.

Additional Joe-Job Information

- The term was first used to describe a spam attack against Joe Doll, webmaster of Joe's Cyberpost, in which a former member of the joes.com website sent a large number of spam emails with the "reply-to" headers forged to make it appear to be from Joe Doll.

- Joe Jobs are acts of revenge and are one of the few spam-related activities that do not have an economic goal.

Recommended Actions

- Apply the Microsoft update associated with the Microsoft Security Bulletin MS08-067 (http://www.microsoft.com/technet/security/Bulletin/MS08-067.mspx) as soon as possible.
- Disable network shares, if possible.
- Monitor network traffic for high to high port activity for randomly generated IP addresses.
- Install antivirus software and keep the virus signatures up to date.
- Disable the Microsoft “Autorun” feature if possible to prevent attack from infection removable media such as USB flash drives or CDs/DVDs.
- Install and keep up-to-date all security patches and software updates for computer’s operating system. If possible, configure the computer to receive automatic software updates from the operating system vendor. If the compute system does not allow automatic updates, manually install the Microsoft security patches as soon as possible from the Microsoft software update website.
- Enable a firewall to filter unwanted traffic from reaching the computer system.
- If an infection is suspected, the computer should be removed from the network.

Conficker Detection Tools

- The U.S. Department of Homeland Security (DHS) announced on Monday, March 30, 2009 the release of a DHS-developed detection tool that can be used by the federal government, commercial vendors, state and local governments, and critical infrastructure owners and operators to scan their networks for the Conficker computer worm. This tool can be provided by Commonwealth Security and Risk Management to State, Local and Higher Educational institutions upon request.

- ISC (Internet Storm Center, www.isc.sans.org) has posted an article on an additional research initiative underway at the Honeynet Project. According to ISC, the Honeynet Project has discovered an anomaly in Conficker that makes it possible to detect infected hosts with an elaborate fingerprint scan over the network. This discovery can be used to detect an infection over the network without the need to physically access each computer on the network. More information on the Honeynet scanner can be found at: http://honeynet.org/node/388. ISC is also reporting that a Nessus Plug-in (Nessus Plug-In 36036) is now available for network scanning. More information can be found at www.nessus.org.

Additional Conficker Detection Tools

- nmap
  - nmap 4.85BETA5 now includes Conficker detection http://insecure.org/
- Nessus
  - http://www.nessus.org/plugins/index.php?view=single&id=36036
- McAfee
  - http://www.mcafee.com/us/enterprise/confickertest.html
- eEye
  - http://www.eeye.com/html/downloads/other/ConfickerScanner.html

Conficker Removal Instructions

- Microsoft
  - http://support.microsoft.com/kb/962007
- Kaspersky
  - http://support.kaspersky.com/faq/
- BitDefender
  - http://www.bitdefender.com/VIRUS-1000462-en--Win32.Worm.Downadup.Gen.html
- TrendMicro
  - http://www.trendmicro.com/vinfo/virusencyclo/default5.asp

Conficker Removal Tools

- To be able to access Anti-Virus vendors from an infected Conficker.C machine, TrendMicro suggests to use "net stop dnscache" from the command line.

- Microsoft MSRT
  - http://www.microsoft.com/security/malwareremove/default.mspx

- F-Secure
  - ftp://ftp.f-secure.com/anti-virus/tools/beta/f-downadup.zip

- Symantec
  - http://www.symantec.com/business/security_response/writeup.jsp?docid=2009-011316-0247-99

- McAfee
  - http://vil.nai.com/vil/conficker_stinger/S.T.I.N.G.E.R.exe

Additional Conficker Removal Tools

- ESET
  - http://download.eset.com/special/EConfickerRemover.exe
- BitDefender
  - http://www.bdtools.net/
- Kaspersky
  - http://data2.kaspersky-labs.com:8080/special/KidoKiller_v3.3.3.zip
- TrendMicro
  - http://www.trendmicro.com/download/dcs.asp

Additional Security Measures

- Implement a “Client-Only” or “Established/Related” traffic filtering list on all Internet-facing firewalls.
  - Allow only the inbound network traffic that is needed.
  - Define the programs, protocols and ports that should have access to the company network.
  - Block unsolicited traffic from connecting to the company network.
  - Prevent LAN traffic from leaving the company network.
  - Filter all inbound traffic with a source IP-address in the RFC-1918 Private IP-address range.
  - Filter all inbound traffic with a source IP-address that matches the IP-address range used on the company network.
  - Consider blocking inbound traffic to TCP-port 135, 139, and 445.
- Enable the “automatic update” feature if one exists for the firewall.
- Firewalls should be configured to log activity. These logs should be reviewed at least once a month to identify any anomalous or unexpected activity.

Additional Security Measures

- To protect the Operating System:
  - Enable the “Automatic Software Update” feature.
  - Remove software that is no longer needed.
  - Remove trial software once the trial has ended.
  - Do not install unsolicited software from any source.

- Turn off File Sharing, Print Sharing, NetBios or other services that are not needed. \

- Employ the Least Privilege concept
  - Create a separate account for system administration on the computer system.
  - Do not use the name Admin, Superuser, Root, or any other term that would suggest that the account is the Administrator account. The “Administrative” account should only be used to install software and make system modifications.

- Create separate accounts for each user on the computer system. The user accounts should be used for the day to day activities. Limiting access to the system privileges associated with the Administrator account will prevent some of the malicious content spreading across the Internet from getting installed on the computer system.

Additional Security Measures

- Every computer system on the network needs an up-to-date version of anti-virus, anti-spyware, anti-spam, and anti-phishing software.
- Configure the Anti-X software to check for product updates on a daily basis.
- Configure the Anti-X software to scan the entire contents of the hard drive at least once a week.
- Configure the Anti-X software to scan ALL removable media each time the removable media is attached to the computer system.
- Monitor the computer system:
  - Monitor hard disk space to determine if the available space decreases for an unknown reason – This may indicated a backdoor has been installed on the computer system and the system is storing information for a malicious individual.
  - Monitor the log files and Event Viewer logs for unexpected error messages
- Renew the software update license each year or purchase a new copy of the software at the end of each year. Do not let the Anti-X software expire.

Conficker-Specific URLs

- Conficker Working Group
  - http://www.confickerworkinggroup.org
- Microsoft End user/Consumer page
  - http://www.microsoft.com/protect/computer/viruses/worms/conficker.mspx
- Microsoft IT Security/Professional Page
  - http://technet.microsoft.com/en-us/security/dd452420.aspx
- ShadowServer
  - http://www.shadowserver.org/wiki/pmwiki.php?n=Calendar.20090212
- Symantec
  - https://forums.symantec.com/t5/Malicious-Code/Coalition-Formed-in-Response-to-W32-Downadup/ba-p/388129

More Conficker-Specific URLS

- Arbor networks
  - http://asert.arbornetworks.com/2009/02/the-conficker-cabal-announced/
- ICANN
  - http://www.icann.org/en/announcements/announcement-2-12feb09-en.htm
- SecureWorks
  - http://www.secureworks.com/research/threats/downadup-removal/
- SRI
  - http://mtc.sri.com/Conficker/contrib/scanner.html
- MNIN Security Blog
  - http://mnin.blogspot.com/2009/01/downatool-for-downadupbconflickerb.html
- Honeynet
  - https://www.honeynet.org/files/KYE-Conficker.pdf

Security Research URLs

- Commonwealth of Virginia Security Information Resource Center
  - Includes security topics within the COV government
  - Addresses topics for those with interests in the security community
  - Summary threat data for public viewing
  - Detailed threat data available for appropriate parties
  - http://www.csirc.vita.virginia.gov

- Commonwealth of Virginia Information Technology Resource Management Policies, Standards, and Guidelines
  - http://www.vita.virginia.gov/library/default.aspx?id=537#securityPSGs

- Commonwealth of Virginia Information Security Awareness Toolkit
  - http://www.vita.virginia.gov/security/default.aspx?id=5146

Additional Security Research URLs

- Internet Storm Center
  - http://isc.sans.org/
- SANS Reading Room
  - https://www.sans.org/reading_room/
- US-CERT
  - http://www.us-cert.gov
- Security Focus
  - http://www.securityfocus.com/
- Team Cymru
  - http://www.team-cymru.org/

Final Thoughts

- The security of the network is ultimately decided by how the computer systems are used.
- It is the responsibility of the computer system owner to protect the network and the computer systems attached to that network.
- A “Fully-Patched” computer system is only fortified against known vulnerabilities. “Zero-Day” exploits and unpublished vulnerabilities can still have a negative impact on the computer systems.
- Scan the computer system for malicious software at least once a week.
- Keep the software on the computer systems up-to-date.
  - Install the latest security updates from the software vendor.
  - Enable Automatic Updates for the operating system, anti-virus, and user applications.

Questions???

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

Thank You!

Virginia Information Technologies Agency

Upcoming Events

UPCOMING EVENTS! IS Orientation

IS Orientation

Monday, May 4th, 9:00 a.m. to 12:00 p.m. (Virginia Highlands Community College, Abingdon, VA)

Information Security Orientation is a small group exploration of Information Security in the Commonwealth focusing on the COV Information Security Policy and Standards and is open to all Commonwealth state and local government persons interested in Information Security.

Register Online for this and future dates at:
http://www.vita.virginia.gov/registration/Session.cfm?MeetingID=0

UPCOMING EVENTS! IS Council

Commonwealth Information Security Council

Monday, May 18th, 12:00 - 2:00 p.m. @ CESC with Committee meetings from 2:00 – 3:00 p.m.

If you would like to attend or be on the agenda for either the Council meeting or a Committee meeting please either contact a Committee co-chair or send an email to CommonwealthSecurity@VITA.Virginia.Gov (not vendors please)

Find out more about your Commonwealth Information Security Officer's Council at: http://www.vita.virginia.gov/security/default.aspx?id=5128

UPCOMING EVENTS! Future 2009 ISOAG's

All currently from 1:00 – 4:00 pm at CESC

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

Wednesday, May 20th

Wednesday, June 17

Tuesday, July 14

Wednesday, August 12

Register Online at:

http://www.vita.virginia.gov/registration/Session.cfm?MeetingID=3

FACTA Red Flag Requirements

Implementation Date: May, 2009

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

Information Systems Security Association

ISSA Central Virginia Chapter Meeting

Topic: Enterprise Data Protection Tech

Presenter: Ulf Mattsson, CTO, Protegrity

Date: May 13, 2009

Cost: ISSA Members: $10
Non-Members: $20

Time & Location: http://www.issacentralva.org/meetings.html

SANS IT Audit Training

Audit 429: IT Audit Essentials Bootcamp Training
At: Virginia Tech Campus
When: May 18-19, 2009, 8am to 7pm

Sign up today to get exceptional *hands-on* security audit training bootcamp style!

Contact Randy Marchany at marchany@vt.edu with any questions.

Event Link and Registration at http://www.sans.org/info/40103

SANS Management Training

Management 414: SANS(R) + S(TM) Training Program for the CISSP(R) Certification Exam

Where: University of Virginia, Charlottesville
When: June 2, 2009

Sans Mentor Marty Peterman will be leading the class.

Complete course details can be found at:
http://www.sans.org/info/442198

UPCOMING EVENTS: MS-ISAC Webcast

National Webcast!

Wednesday, June 17, 2009, 2:00 to 3:00 p.m.

Topic: Securing Mobile Devices

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, June 23

8:30 am – 9:00 am: Networking

9:00 am: Meeting start

Location: Department of Health Professions
Perimeter Center, 9960 Mayland Drive
2nd floor conference center

Any Other Business ??????

ADJOURN

THANK YOU FOR ATTENDING!!