



# Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

September 13, 2007



# ISOAG August 2007 Agenda

- |       |   |   |
|-------|---|---|
| I.    | Welcome   | Peggy Ward  |
| I.    | Opening Remarks   | Dr. Sandra G. Treadway, Librarian of Virginia   |
| II.   | Basic Records Management                                  | Amy Judd, Library of Virginia   |
| II.   | Commonwealth Document Management Initiative               | Herb Ward & Bernie Farkas, Department of Environmental Quality                          |
| IV.   | Protection of Personally Identifiable Information         | Lisa Wallmeyer, Executive Director, Virginia Joint Commission on Technology and Science |
| V.    | Data Breach Notification                                  | Peggy Ward, VITA  |
| VI.   | Introduction to IT Infrastructure Transformation          | Tony Shoot & Mike von Slomski, Commonwealth IT Infrastructure Partnership               |
| VII.  | Desktop Image/Application Security & VAR Approval Process | Monty Frahm & Todd Kissam, VITA   |
| VIII. | Local Admin Rights  | Cathie Brown, VITA  |
| IX.   | Honeypots   | Tripp Sims, VITA  |
| X.    | Upcoming Events & Other Business                          | Peggy Ward, VITA  |



# Internet Safety & Cyber Security Months

## **HOUSE JOINT RESOLUTION NO. 587**

**Designates September 2007 & each subsequent September as Internet Safety Month!**

**Governor Kaine has proclaimed October to be Cyber Security Awareness Month for the Commonwealth!  
We have one proclamation for each agency or locality attending today!**

**Celebrate! Have an event! Give tips! Hand out reminders!**

# Opening Remarks

**Dr. Sandra G. Treadway**  
**Librarian of Virginia**

# Records Management 101

## **The Basics**

**Amy Judd**  
**Archival and Records**  
**Management Services Division**



# What is a Record?

"Public record" or "record" means recorded information that documents a transaction or activity by or with any public officer, agency or employee of an agency. Regardless of physical form or characteristic, the recorded information is a public record if it is produced, collected, received or retained in pursuance of law or in connection with the transaction of public business. The medium upon which such information is recorded has no bearing on the determination of whether the recording is a public record.

**Code of Virginia, Title 42.1 Chapter 7**  
*Virginia Public Records Act*

# What is a record REALLY?

## **A RECORD:**

- Documents a transaction or activity
- Includes **all mediums** regardless of physical form or characteristic
- And is considered a **public record** if it is produced, collected, received or retained in pursuance of law or in connection with the transaction of public business

# Vital Records . . .

**Vital Records** are those records essential to the operation of the organization and/or resumption of operations following a disaster. These are records that you must have to stay in business, such as accounts receivable, patents, current patient files, or payroll records.

# What is not a record?

- **Reference materials:**
  - reference texts, magazine and newspaper articles, textbooks, presentation handouts, extra copies of official records, etc.
- **Administrative and personal correspondence/e-mail:**
  - meeting times, lunch dates, staff association memos, FYI memos, spam, etc.
- **Personal materials:**
  - errand lists, bills, checkbooks, personal letters and/or photos, etc.
- **Stationary, blank forms, and publications for distribution**
- **Copies of policy and procedure manuals**

# The Commonwealth

- Minimize litigation risks
- Ensure federal, state, and regulatory compliance
- Safeguard vital information



# The Agency



*Virginia Department of  
Employment Dispute Resolution*



- Ensure business continuity
- Support decision making
- Preserve the corporate memory

# The Employees

- Control the growth of records
- Improve efficiency and productivity
- Integrate new Records Management technologies



# Records management is...

Providing the right information

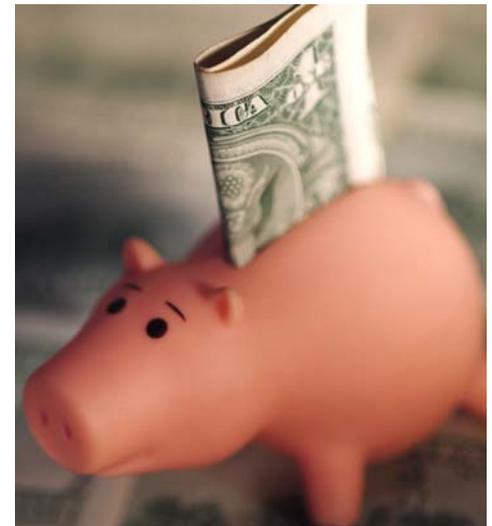
At the right time

To the right people

Effectively & efficiently



At the  
lowest possible cost.



# From Record Series to Record Schedule

## Record Series

Documents normally filed together because they result from the same activity or relate to a particular function

## General Schedule

Common records created and maintained by localities and state agencies

## Specific Schedule

Records unique to an agency and reflects its responsibilities

[http://www.lva.lib.va.us/whatwedo/records/sched\\_state/index.htm](http://www.lva.lib.va.us/whatwedo/records/sched_state/index.htm)



**What We Do**

[What We Have](#)

[Who We Are](#)

## State Agency General Schedules

[Introduction](#)

[Glossary](#)

[Searchable Database for State General Schedules](#)

[GS-101](#), Administrative Records (Jan 06) \* **Series 100381 Deleted \***

[GS-102](#), Fiscal Records (Jan 03)

[GS-103](#), Personnel Records (Mar 06) \* **Series 012172 Revised \***

[GS-104](#), Mailroom Records (Mar 01)

[GS-105](#), Motor Vehicle Records (Apr 01)

[GS-106](#), General Services Records (Sep 00)

[GS-107](#), Food Service Records (May 01)

[GS-108](#), Fire, Safety and Security Records (Sep 05)

[GS-109](#), Library and Museum Records (Aug 01)

[GS-110](#), Electronic Records (Oct 98) (See GS 2000 for Y2K Records)

[GS-111](#), College and University Records (May 01)

GS 112, Community College Records, formerly 261-GS-1, now replaced by [GS-111](#).

[GS-2000](#), Y2K Records (July 99)

**\* Recent Updates Highlighted in Red \***

RECORDS RETENTION AND DISPOSITION SCHEDULE  
GENERAL SCHEDULE NO. 102  
ALL STATE AGENCIES  
FISCAL RECORDS

EFFECTIVE SCHEDULE DATE

PAGE 3 OF 15 PAGES

## RECORDS SERIES AND DESCRIPTION

## SERIES NUMBER

## SCHEDULED RETENTION AND DISPOSITION

Audit Reports – Duplicates

012087

Retain as long as administratively necessary, then destroy.

This series consists of reference/working copies of the audit report.

Bank Records - Payroll Related

012088

Retain 4 years or until audit, whichever is longer, then destroy in accordance with No. 8 on the schedule cover page.

This series documents the agency's financial affairs with a banking institution relating to the payroll.

Bank Records - All Other Bank Records

012089

Retain 3 years or until audit, whichever is longer, then destroy.

This series documents the agency's financial dealing with a banking institution that are non-payroll related.

Batch Headers

Refer to record series 012155, "Vouchers."

This series is used to group, transport, account or process records in batches, usually by electronic means.

Bid Package and Bid Proposals

Refer to records series 012142, "Purchasing-Bid and Bid Proposal Files."

Budget Records-Work Papers/Reports

012092

Retain 3 years after the biennium to which the records relate, then destroy.

This series documents the budgeting procedure of the agency. It consists of working papers relating to the preparation of the budget and reports that deal with the control of expenditures within the agency.

Budget Records-Internal Budget Files

012093

Retain 3 years after the biennium to which the records relate, then destroy.

This series is used by the agency as it deals with its budget during the fiscal year.

# Important Things to Know

1. “Destroy in compliance with No. 8 on the schedule cover page.”
2. If your records do not fall into any series on any General Schedule or your Agency Specific Schedule, it can not be destroyed.
3. Format does not matter. Content does.
4. Retention periods are not suggestions.

# Code of Virginia §42.1-86.1

## IMPORTANT CHANGE TO THE VIRGINIA PUBLIC RECORDS ACT

“C. Each agency shall ensure that records created after July 1, 2006 and authorized to be destroyed or discarded in accordance with subsection A, are destroyed or discarded in a timely manner in accordance with the provisions of this chapter; provided, however, such records that contain identifying information as defined in clauses (iii) through (ix), or clause (xii) of subsection C of §18.2-186.3 shall be destroyed within six months of the expiration of the records retention period.”

### **What does destruction of records in a “timely manner” mean?**

The Library of Virginia interprets “timely manner” to mean that records scheduled for destruction will be destroyed no later than the end of the year (calendar or fiscal) in which the retention period expires.

# Records Destruction Procedure

- Identify what is to be destroyed and how by using retention schedule
- Fill out RM-3 – Interactive form at [www.lva.lib.va.us/whatwedo/records/forms/rm3ia.pdf](http://www.lva.lib.va.us/whatwedo/records/forms/rm3ia.pdf)
- Obtain Designated Official and Records Officer signature
- When records **HAVE BEEN DESTROYED** obtain signature of the individual who destroyed the records or witnessed the destruction.
- Send form with **ALL** original signatures to the Library of Virginia



Archival and Records Management Services Division  
 800 East Broad Street, Richmond, VA 23219-8000  
 (804) 692-3600

# CERTIFICATE OF RECORDS DESTRUCTION

(Form RM-3 May 2007)

This form documents the destruction of public records in accordance with the *Virginia Public Records Act*, § 42.1-76 through 42.1-91 of the *Code of Virginia*.

**INSTRUCTIONS ON BACK**

<b>1. Agency / Locality</b> Library of Virginia	<b>2. Division / Department / Section</b> Archives and Records Management Services	
<b>3. Person Completing Form</b>	<b>4. Address</b>	<b>5. Telephone Number &amp; Extension</b>

**6. Records to Be Destroyed**

a) Schedule and Records Series Number	b) Records Series Title	c) Date Range (mo/yr)	d) Location	e) Volume	f) Destruction Method
GS101; 100355	VPRA booklet design documentation files	1-2007 to 6-2007		.1 cu. ft.	Trashcan
202-027; 005433	Workshop attendance records	1998-2001		.5 cu. ft.	Trashcan
GS101; 012018	Non-routine correspondence	2003-2004		.5 cu. ft.	Trashcan
GS101; 012018	Non-routine correspondence	2003-2004		2MB	Deleted
GS101; 100323	Disaster Recovery grant documentation	2003		4 cu. ft.	Shredded

**DESTRUCTION APPROVALS**

*NOTE: Public records may not be destroyed without receiving prior approval from your agency or locality Records Officer.*

We certify that the records listed above have been retained for the scheduled retention period, required audits have been completed, and no pending or ongoing litigation or investigation involving these records is known to exist.

**7. Approving Official (Print)** \_\_\_\_\_ **Signature** \_\_\_\_\_ **Date** \_\_\_\_\_

**8. Designated Records Officer (Print)** \_\_\_\_\_ **Signature** \_\_\_\_\_ **Date** \_\_\_\_\_

**9. Records Destroyed By (Print)** \_\_\_\_\_ **Signature** \_\_\_\_\_ **Date** \_\_\_\_\_

# Email is not a record series

Email is a format, not a record series. Asking how to file an email is the same as asking how to file a piece of paper.

The content determines the disposition.

# Basic information

- State agency employees are responsible for managing e-mails, including messages sent and received.
- You are responsible for all e-mails you send. Your function within the agency defines whether you keep e-mails you receive.
- Requests from the public for e-mail records, including FOIA requests, must be honored in the same manner as other public records.
- E-mail records must remain accessible during their entire retention period and should be maintained in such a manner as to permit easy access and timely retrieval.

# Organizing E-mails

- Organize e-mail in folders by records series or subject area and fiscal or calendar year.
- Establish agency- or division-wide filing structures.
- “AutoArchiving” within Outlook is not recommended.
- Archive manually and frequently.

## All Mail Folders

- [-] Mailbox - Ariel Billmeier
  - Deleted Items
  - Drafts [1]
  - Inbox
  - Junk E-mail
  - Outbox
  - [-] Saved Items
    - Data Wiping 2006
    - E-Mail Guidelines 2006
    - Governor's E-mail 2006
    - Imaging Standards 2006
    - Instant Messaging & Teleworking 2006
    - IT Schedule 2006
    - LVA 2006
    - Paperless Government 2006
    - Permanent E-Records 2006
    - Records Analysis 2006
    - Redaction Issues 2006
    - Secretary of Technology 2006
    - To Read 2006
    - Travel & Training 2006
    - VITA 2006
  - Sent Items
  - [+] Search Folders

**Folders to  
Archive**



# Secretary of Technology 2006 Properties



Administration

Forms

Permissions

Synchronization

General

Home Page

AutoArchive



Secretary of Technology 2006

Type: Folder containing Mail and Post Items

Location: \\Mailbox - Ariel Billmeier\Saved Items

Description:

Retain two years, then destroy.

Show number of unread items

Show total number of items

When posting to this folder, use: IPM.Post

Automatically generate Microsoft Exchange views

Folder Size...

Clear Offline Items

OK

Cancel

Apply

Specify Retention  
within Folder  
Properties



# Printing E-mail

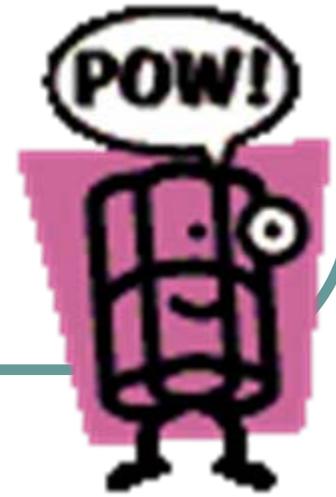
- Names and e-mail addresses of recipients
  - If an e-mail is sent to a distribution list, include names and addresses of all members of distribution list)
- Name and e-mail address of sender
- Time and date sent
- Subject line that describes the content of the e-mail
- Text
- Attachments, if applicable

# Top Five Tips for E-mail Use

- 5) Official “signature”
- 4) Proofread
- 3) Retain final e-mail
- 2) Useful subject line

# Top Five Tips for E-mail Use

1) Do not put anything in an e-mail message that you would not want to see printed in tomorrow's newspaper or displayed on a bulletin board. When sensitive issues need to be discussed, a face-to-face conversation or telephone call may be a better communication choice than e-mail.



# The Library of Virginia can help

The Records Analysis Section provides you, our client, the following support:

- consult in developing and implementing a records management program
- consult in developing, updating, and modifying records series and schedules
- provide training on policies and procedures
- assist with disaster planning and recovery

# State Records Center

The SRC provides the following services:

- storage for inactive non-permanent records (paper, microfilm, and digital media) in a climate controlled facility with secure, controlled access
- pick-up services for storage and shredding within 150 miles of the SRC
- confidential shredding of records – paper, microfilm, and electronic
- degaussing of hard drives
- assist with disaster recovery

# State Laws and Regulations

- *Virginia Public Records Act (VPRA)* [**Code of Virginia § 42.1-76 et. seq.**]
- *Freedom of Information Act (FOIA)* [**Code of Virginia § 2.2-3700 et. seq.**]
- *Government Data Collection and Dissemination Practices Act*  
[**Code of Virginia § 2.2-3800 et. Seq**]
- *Copies of Originals as Evidence*  
[**Code of Virginia § 8.01-391**]



THE LIBRARY OF VIRGINIA

## **Archives and Records Management**

### **Services Division**

800 E. Broad Street

Richmond, Virginia 23219

Phone: 804-692-3600

Fax: 804-692-3603

Or search our website at:

<http://www.lva.lib.va.us/whatwedo/records/index.htm>

---

# Enterprise Document Management Initiative

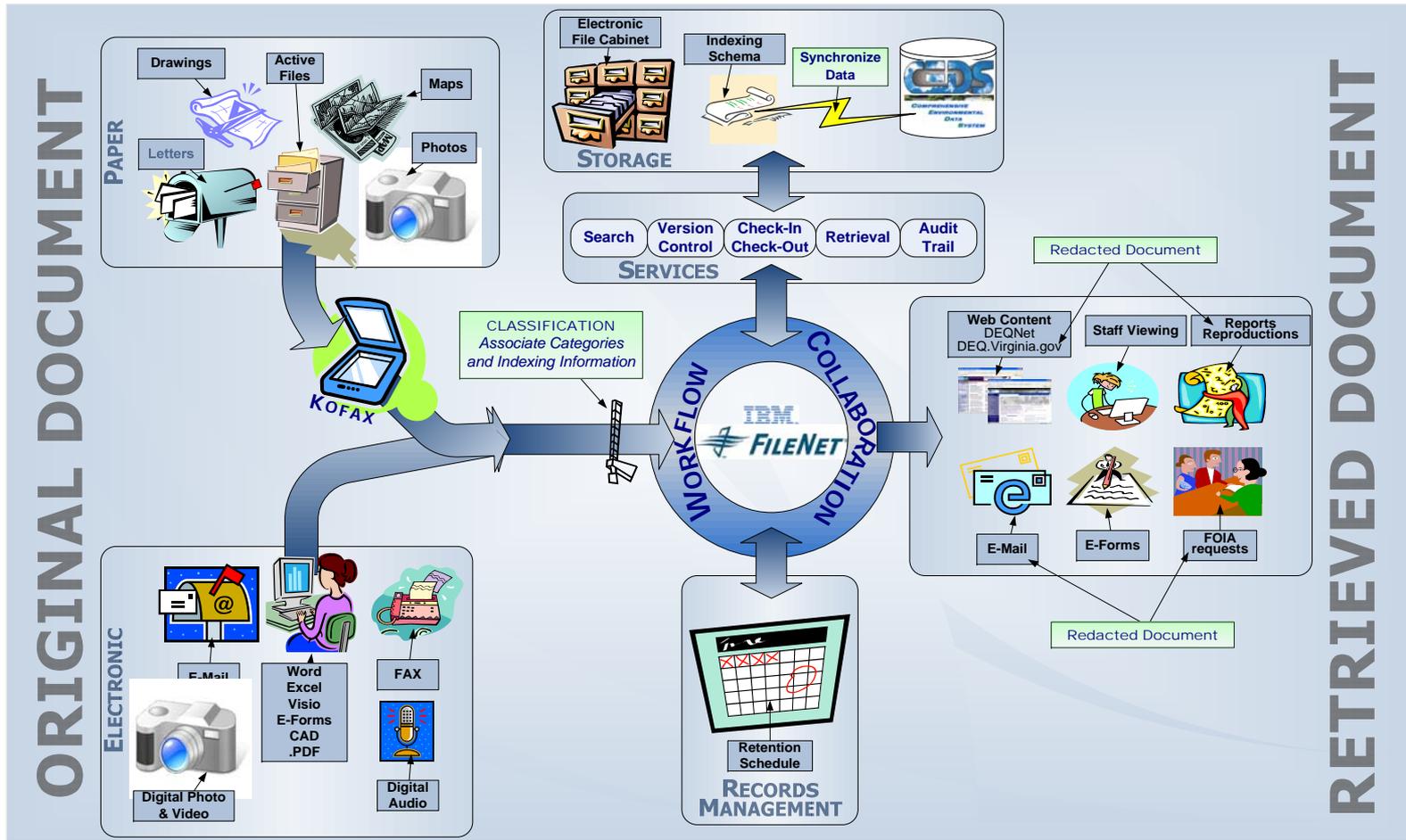
---

Presented by

- Herb Ward
- Bernie Farkas



# What is an Enterprise Content Management System?



---

# Goals and Objectives

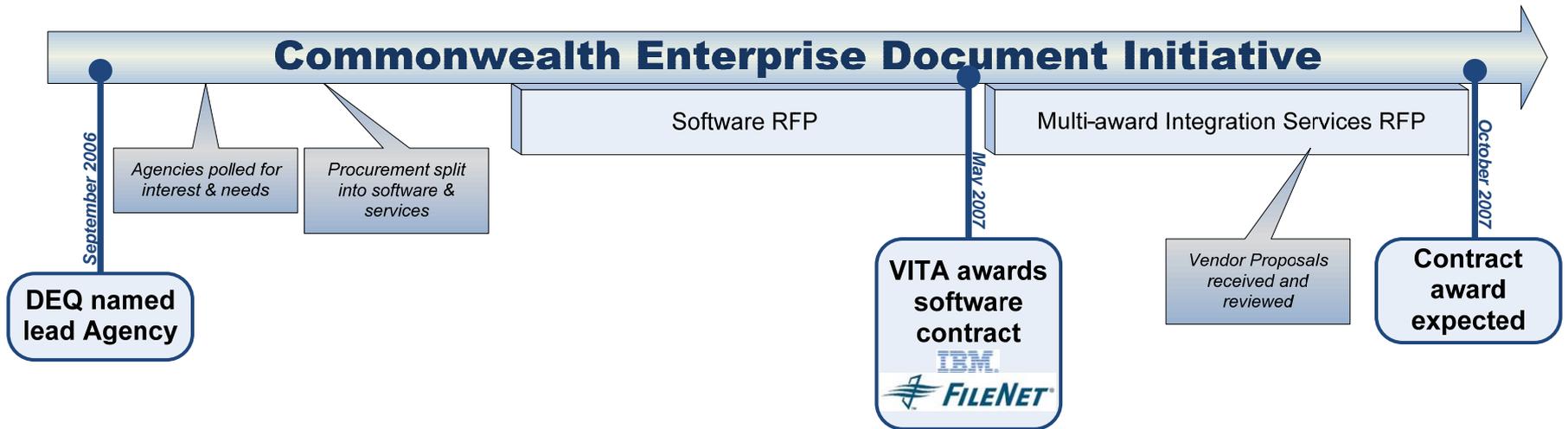
- Streamlined Procurement Process for Commonwealth Agencies
    - IBM-FileNet contract enables an Agency to select necessary components without an RFP process
    - Integration Services contract enables an Agency to issue a Statement of Work to any vendor on the contract
  - Commonwealth Governance
    - Sharing of experiences and best practices
    - Leveraging customized development
    - Guidance to 'Paperless Government'
-

# “Paperless” Government Initiative

Evaluation Teams		
Agency	Software	Integration Services
Department of Environmental Quality	✓	✓
Department of Juvenile Justice	✓	✓
Department of Social Services	✓	
Department of Transportation	✓	✓
Library of Virginia	✓	✓
Virginia Information Technology Agency	✓	✓
Virginia Retirement System	✓	

- DEQ is the lead agency for the statewide procurement of ECM Software and Implementation Services

# Timeline of ECM Procurement



---

# Questions?

- Herb Ward

- 804.698.4316

- [hrward@deq.virginia.gov](mailto:hrward@deq.virginia.gov)

- Bernie Farkas

- 804.698.4386

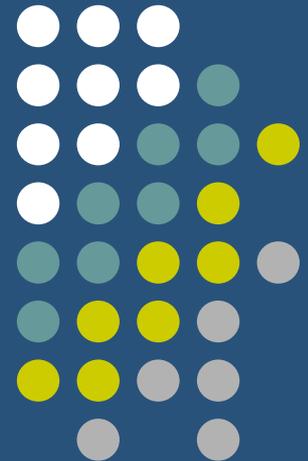
- [bwfarkas@deq.virginia.gov](mailto:bwfarkas@deq.virginia.gov)

---

# Virginia Joint Commission on Technology and Science

Protection of Personally Identifiable  
Information

Lisa Wallmeyer, Executive Director





# What is JCOTS?

- JCOTS is a permanent legislative commission, established by the General Assembly in 1997 to...

“...study all aspects of technology and science and endeavor to ***stimulate, encourage, promote, and assist*** in the development of technology and science in the Commonwealth and sound public policies related thereto...”

(§ 30-85 of the Code of Virginia)

# Personal Identifying Information



- 2007 General Assembly referred two bills to both JCOTS & the Freedom of Information Advisory Council:
  - Both bills would create a FOIA exemption to allow personal identifying information to be withheld from public disclosure
  - One bill would just exempt Social Security Numbers
  - One bill would exempt Social Security Numbers, financial information, and other personally identifiable information

# Joint FOIA/JCOTS Meetings



- Representatives from both organizations have met twice
- Examined issues relating to current treatment of SSN/personally identifiable information in the Code
- Key question emerged: What data are our state agencies collecting? Are we collecting just what we need? More than we need? Are agencies collecting SSN in situations where it's not protected?



We need help understanding  
what data is being regularly  
collected by our state  
agencies



# Further Information

Information, reports, agendas, meeting materials, etc. can be found on the JCOTS website: <http://jcots.state.va.us>

910 Capitol Street  
General Assembly Building, 2d Floor  
Richmond, VA 23219  
(804) 786-3591  
[jcots@leg.state.va.us](mailto:jcots@leg.state.va.us)



# Date Breach Notification

Peggy Ward

---





## COV ITRM Standard SEC501-01 Section 9.5.2 #'s 3-6

### What?

Early adoption of 9.5.2 Data Breach Notification, #'s 3-6

### Why?

Borne of participation in the Governor's Working Group for Executive Directive No. 5 – Requested by Delegate Plum to pave the way for comprehensive data breach legislation in Virginia by leading the way!

### When?

Motion to be recommended to the Commonwealth Information Technology Investment Board @ October meeting for Compliance effective November, 2007



## COV ITRM Standard SEC501-01 Section 9.5.2 #'s 3-6

**Applies to: Personally Identifiable Information (PII) which means Name and any of the following:**

- Social Security Number
- Drivers license or Identification card number
- Financial account number, credit or debit card number
- Other personal identifying information, such as insurance data or date of birth.



## COV ITRM Standard SEC501-01 Section 9.5.2 #'s 3-6

### 9.5.2 Data Breach Notification

3. Provide appropriate notice to affected individuals upon the unauthorized release of unencrypted PII by any mechanism, including, but not limited to:
  - a. Theft or loss of digital media including laptops, desktops, tablets, CD's, DVD's, tapes, USB drives, SD cards, etc.;
  - b. Theft or loss of physical hardcopy; or
  - c. Security compromise of any system.

The agency shall provide this notice without undue delay as soon as verification of the unauthorized release is confirmed, except as delineated in #6, below.

4. Provide notification that consists of:
  - a. A general description of what occurred and when;
  - b. The type of PII that was involved;
  - c. What actions have been taken to protect the individual's personal information from further unauthorized disclosure;
  - d. What, if anything, the agency will do to assist affected individuals, including contact information for more information and assistance; and
  - e. What actions the agency recommends that the individual take.



## COV ITRM Standard SEC501-01 Section 9.5.2 #'s 3-6

5. Provide this notification by one or more of the following methodologies, listed in order of preference:
  - a. Standard mailing to any affected individuals whose mailing addresses are available.
  - b. Electronic mail to any affected individuals whose email address has been provided to the agency as a contact mechanism.
  - c. In the case of large scale breaches or data breaches where neither form of communication listed above is available or feasible, public communications channels, including:
  - d. Conspicuous notification on the agency website; and
  - e. Notification by statewide public media, including newspaper, radio, and television).
  
6. Not provide notification immediately following verification of unauthorized data disclosure only if requested by:
  - a. Law Enforcement entities where it would interfere with an ongoing investigation; or
  - b. CISO or designee where it would interfere with a determination of the scope of the data breach or investigation of root cause.



# Date Breach Notification

??

??Questions??

??



# Introduction to IT Infrastructure Transformation

Northrop Grumman IT  
*Transformation Projects Team*

**Tony Shoot & Mike von Slomski**  
**Commonwealth IT Infrastructure Partnership**



**NORTHROP GRUMMAN**

## Agenda

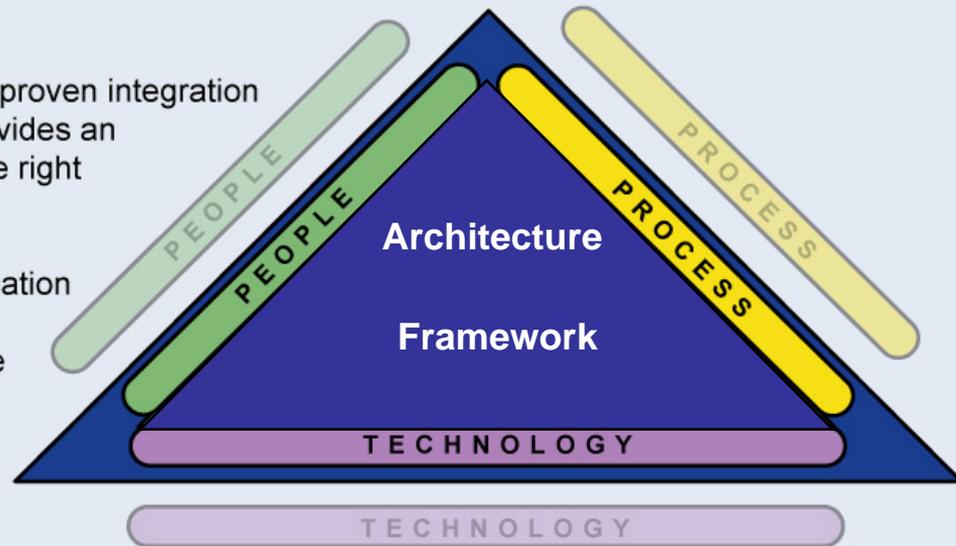
- Architecture Elements
- Transformation Overview
  - Overview
  - Deployment Approach
  - Team Structure and Roles
  - Next Steps
- Roll-out Plan
- Transformation Status
- Questions

# Architecture Elements

---

# People Process and Technology

- The Information Technology Service Management (ITSM) methodology is built on the integration of People, Process and Technology
- The Northrop Grumman Team's proven integration of these 3 main components provides an efficient method for delivering the right service at the right time
- As a framework providing Information Technology Structure, Rules and Governance, the VITA Enterprise Architecture's "gravity" pulls together the ITSM components providing a solid foundation in which to define, build and deliver solutions



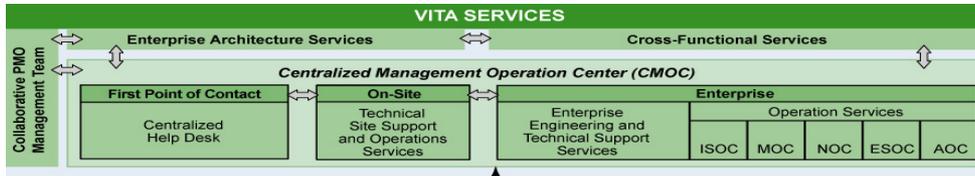
VITA 177\_r5

**The VITA enterprise architecture's "gravity" pulls together the ITSM components, providing a solid structure in which to define, build, and deliver solutions.**



NORTHROP GRUMMAN

# Transformed Service Solutions Model



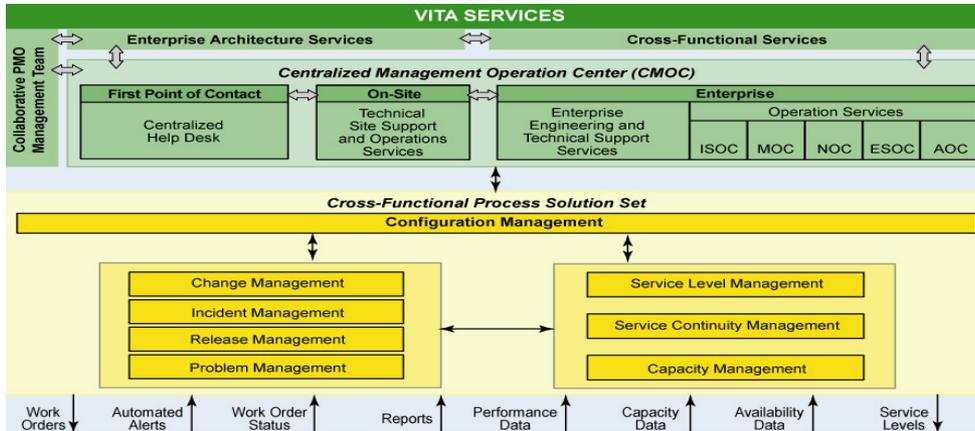
PEOPLE

Service Delivery Organization



NORTHROP GRUMMAN

# Transformed Service Solutions Model



PEOPLE

Service Delivery Organization



PROCESS

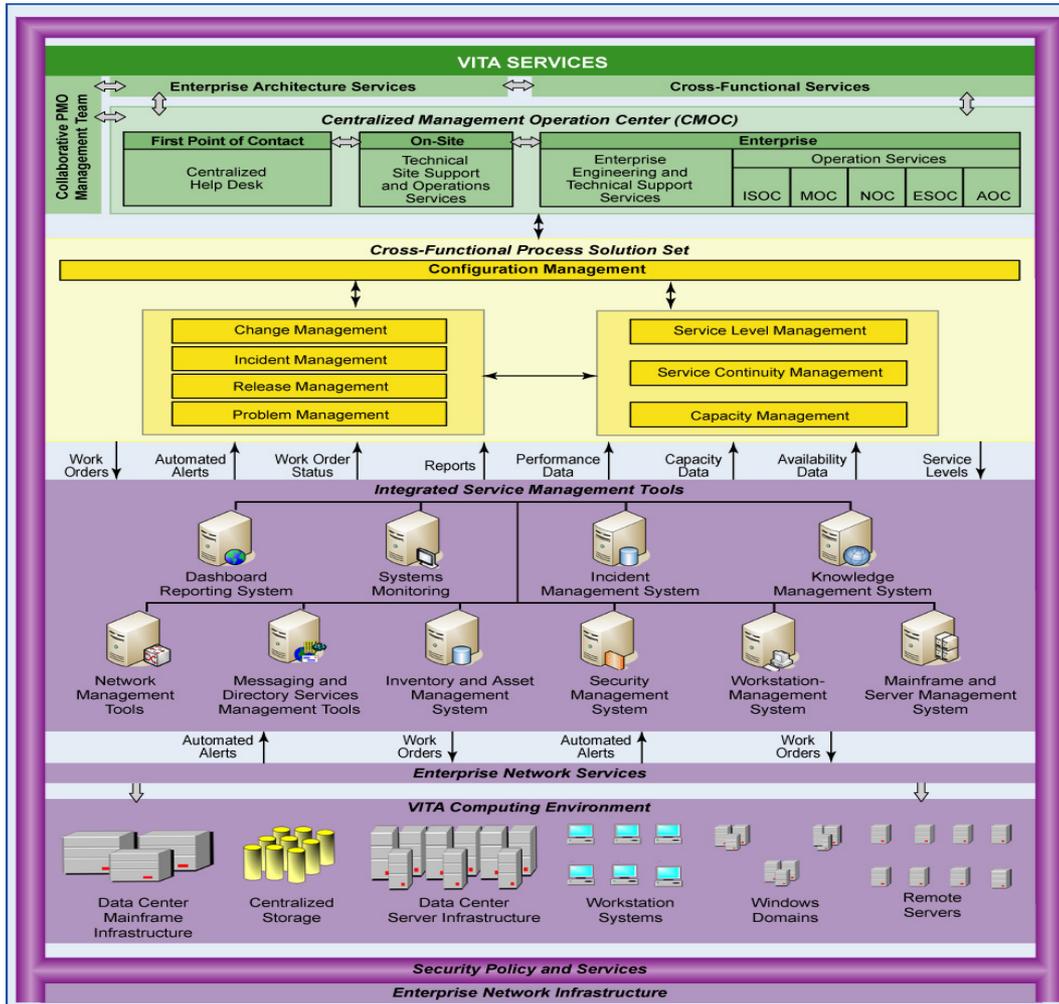
Service Management

Operations Management



NORTHROP GRUMMAN

# Transformed Service Solutions Model

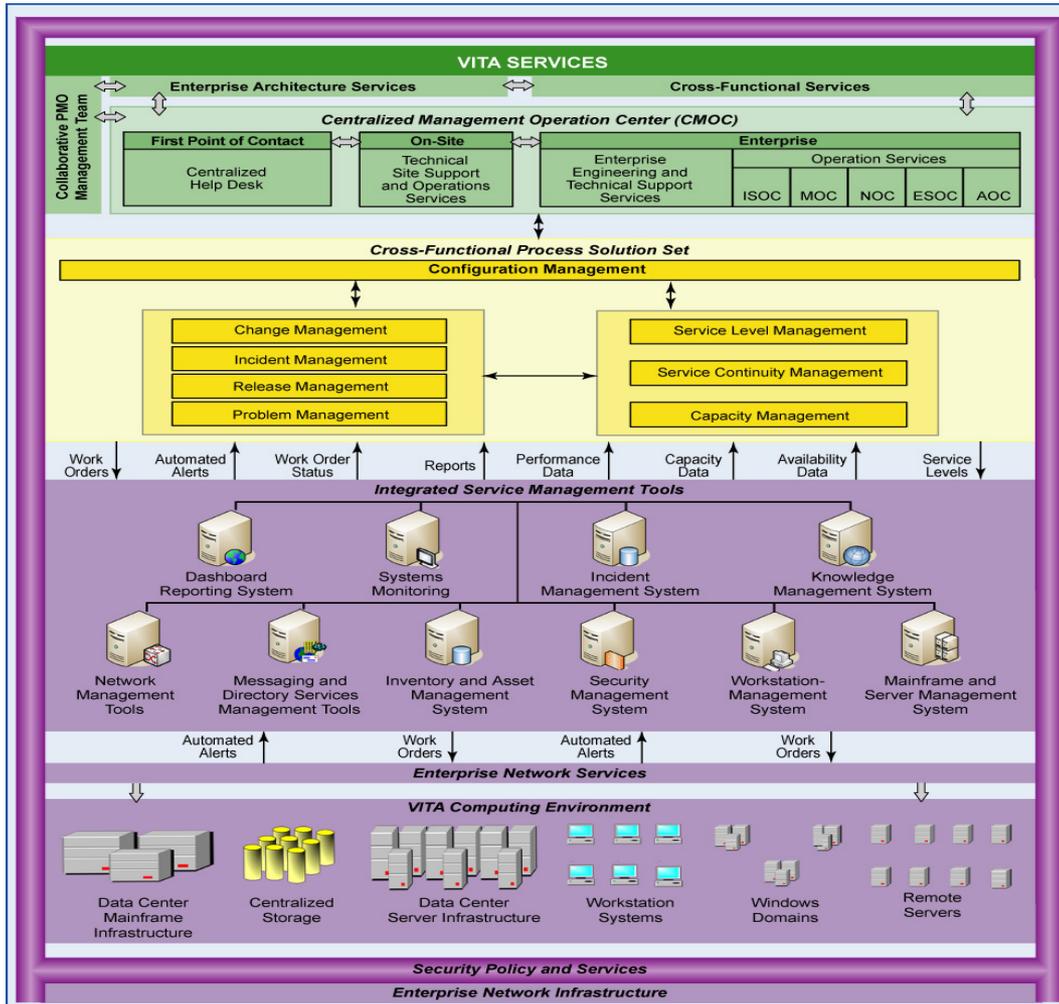


- 
**PEOPLE**  
 Service Delivery Organization
- 
**PROCESS**  
 Service Management  
 Operations Management
- 
**TECHNOLOGY**  
 Service / Systems Mgmt Infrastructure  
 Computing Infrastructure  
 Network Infrastructure & Services  
 Security Infrastructure & Services  
 Directory Service Infrastructure & services  
 Messaging Infrastructure & Services  
 LOB Application Infrastructure & Services

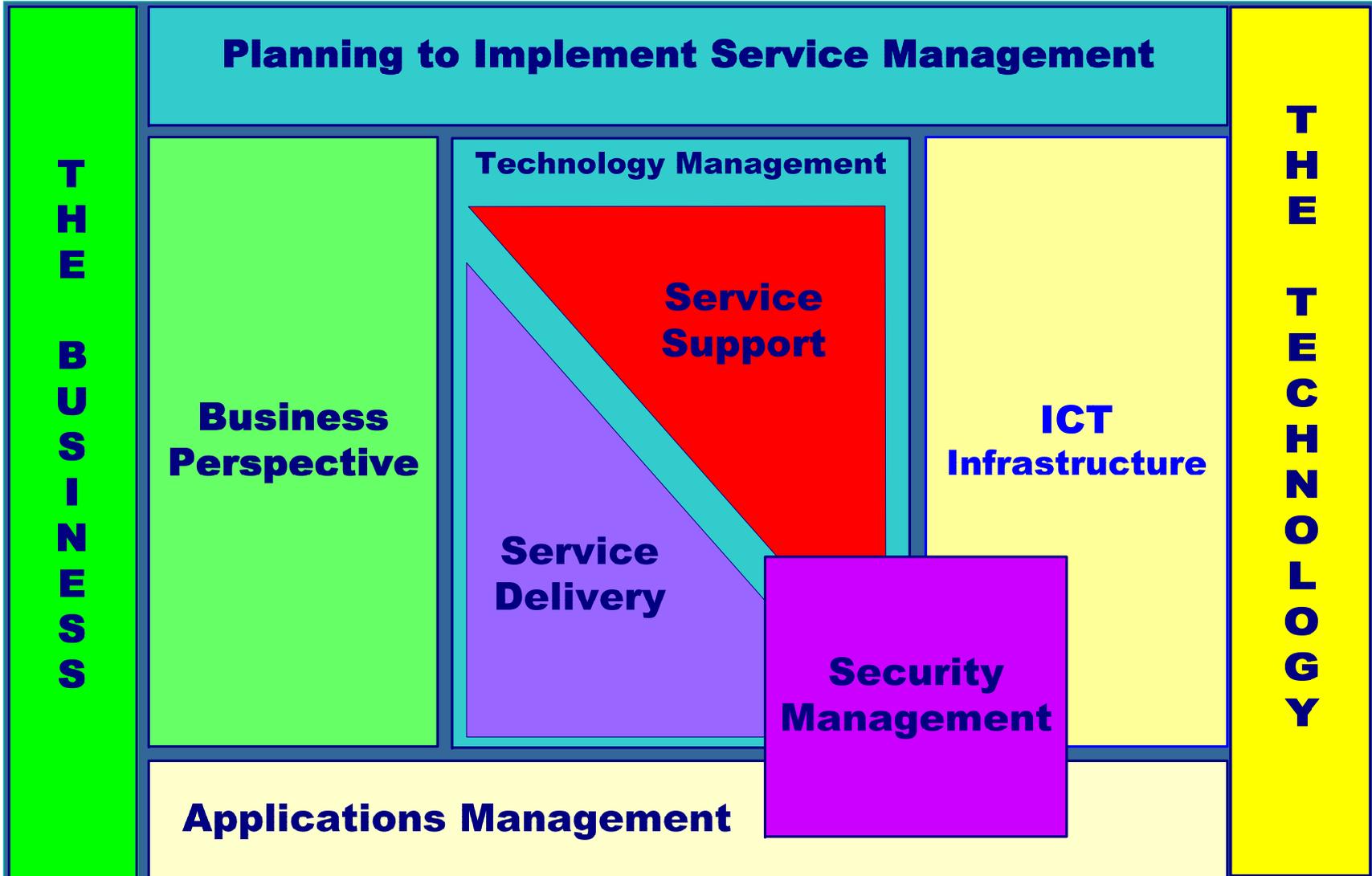


NORTHROP GRUMMAN

# Transformed Service Solutions Model

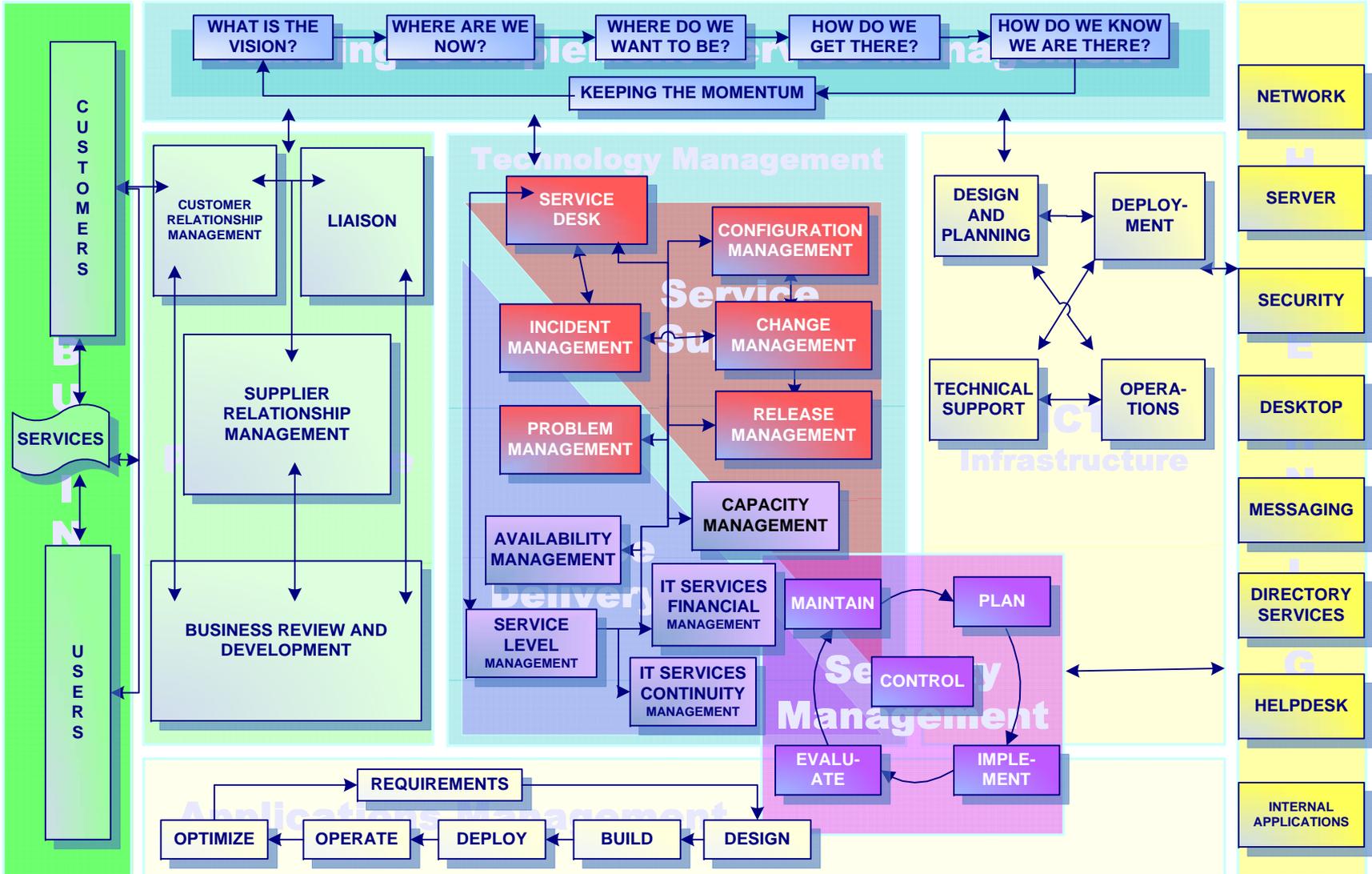


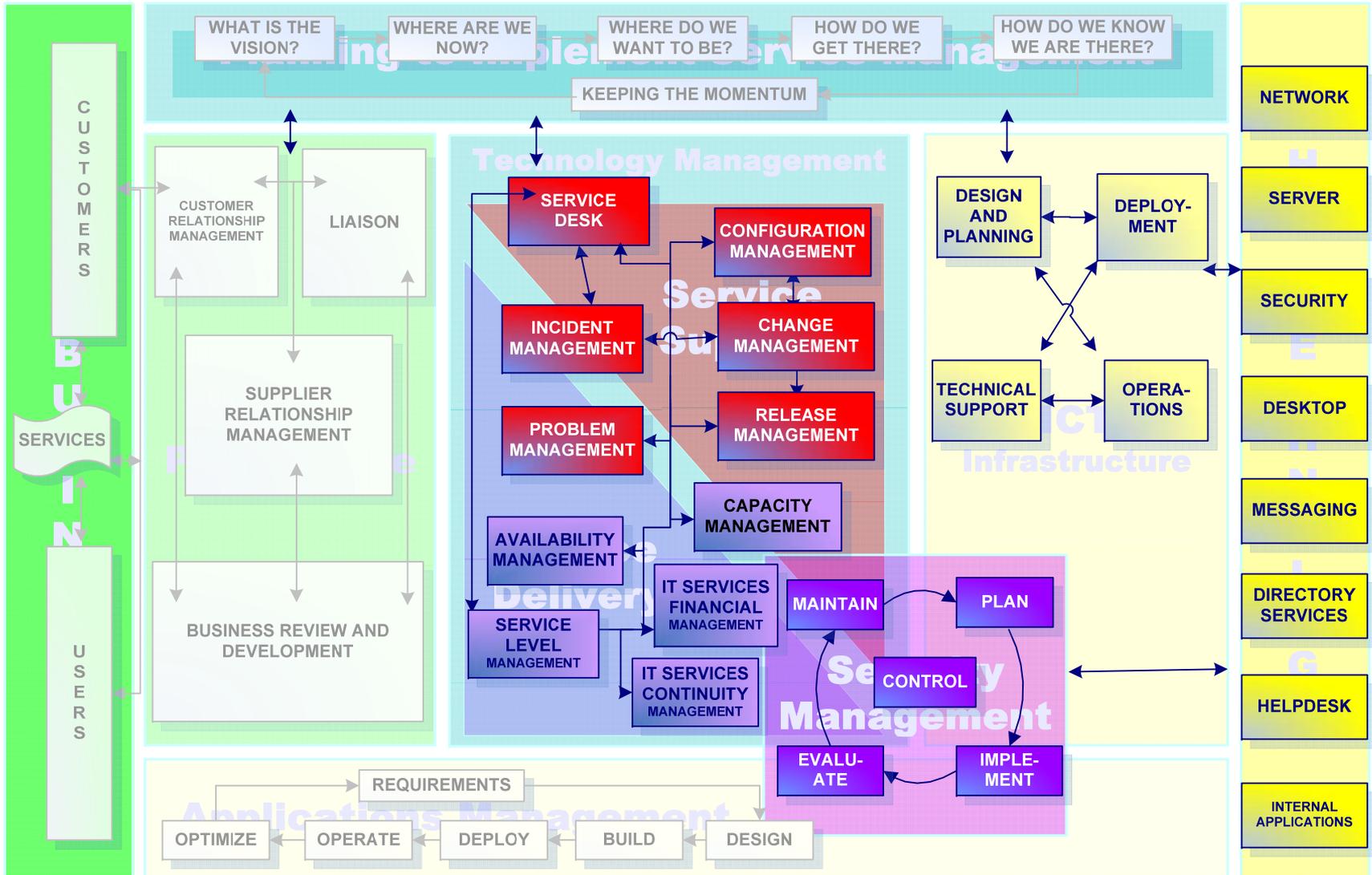
- 
**PEOPLE**  
 Service Delivery Organization
- 
**PROCESS**  
 Service Management  
 Operations Management
- 
**TECHNOLOGY**  
 Service / Systems Mgmt Infrastructure  
 Computing Infrastructure  
 Network Infrastructure & Services  
 Security Infrastructure & Services  
 Directory Service Infrastructure & services  
 Messaging Infrastructure & Services  
 LOB Application Infrastructure & Services





NORTHROP GRUMMAN







# Service Management Product Summary

INTENTIONALLY OMITTED

# Service Management Product Summary

INTENTIONALLY OMITTED

# Service Management Product Summary

INTENTIONALLY OMITTED

# Transformation Project Summary

INTENTIONALLY OMITTED

# Transformation Project Summary

INTENTIONALLY OMITTED

# Transformation Overview

---



NORTHROP GRUMMAN

# Purpose

## Previous Communications

## Current Purpose

**VITA Virginia Information Technologies Agency**

**Key Points to Start**

- Transformation = Better Services: The Commonwealth will get a 21<sup>st</sup> century IT infrastructure for what it's paying to maintain a 1980s IT infrastructure
- No Inflation: VITA will not be receiving today for services in question
- VITA Employees: It is our intent to accomplish the retirement, retraining, and redeployment of VITA employees

**Implementation Timeline**

**Transformation Projects**

<b>Help Desk</b> Enterprise Help Desk in Labaron and Meadowville Field Based agents and technicians for Level 3 Enterprise Help Desk System (Pyeongta)	<b>End User Services (EUS) Desktop</b> Mass Desktop Refresh Project Network Printer Consolidation and Refresh Enterprise Code Enterprise Desktop Management Systems	<b>Messaging</b> Enterprise Exchange Enterprise Code Active Directory
<b>Mainframe and Servers</b> New IBM and Unisys Mainframes in new Data Center Consolidation and refresh of servers Migration of servers to the data center	<b>Data Center Services (DCS) Facilities</b> New Data Center/Office Building in Meadow New Disaster Recovery Center and Help D in Labaron/Russell County	
<b>Network</b> New Commonwealth wide MPLS Core WAN LAN upgrades to local switches/routers as needed Network re-addressing of IP	<b>Network Services (NWS) Voice / Video</b> Voice over IP Network optimized for voice and video traf	
<b>Security Services (SS) Security</b> Enterprise Security Operations Center Computer Security Incident Response Center Secure Internet Gateway		

**Value of VITA 2006**

**IT Transformation**  
Bringing 21<sup>st</sup> Century Technology to the Business of Government

**The Case for Change**

Virginia state government is a \$34 billion per year business, the equivalent of a Fortune 50 company. The Commonwealth's current information technology (IT) infrastructure, however, would not keep a Fortune 50 company in business for very long. Consider the following deficiencies:

**Inadequate Security and Back-Up**

- Current Executive Branch data networks are a mixed bag of overlapping, often redundant systems with varying levels of security protection and no comprehensive capability to detect and proactively react to other attacks.
- State government data centers have multiplied to more than 100 locations. Some are no more than storage closets, and many are without adequate security, fire protection, and back-up power.
- Many state agencies' mission-critical systems lack adequate disaster recovery capabilities.

**Lack of Capabilities**

- More than 70 agencies currently provide an IT help desk of some sort. In addition to needless duplicating services, most lack even basic problem diagnosis and response tools to determine and fix root causes, not just address symptoms.
- Some agencies even lack basic office automation tools that one would expect to find today in any business of any size.

**IT Investment**

	From Present State	To Future State
Network	Fragmented	Integrated
Security	Inadequate	Adequate
Servers	Numerous locations, none capacity (2,000+)	Consolidated (<1,000)
Computing	Inconsistent	Standardized
Help desk support	Multiple (70+)	Combined (1)
Service levels	Undefined performance	Defined

Under the best of circumstances, even the most important state-wide business applications cannot be recovered at an off-site location in less than three days.

The overall state of Virginia state government's current, decentralized IT environment has come about despite the dedicated efforts of individual agencies



- Review elements of the IT infrastructure to be transformed
- Present Transformation deployment approach
- Discuss roles & responsibilities for deployment
- Solicit feedback

High-level information about Transformation

Transformation as the agencies will experience it

# Contents

## Transformation Overview

- ▶ Description of Transformation
- ▶ Key Elements & End State
- ▶ Benefits of Transformation

## Deployment Approach

- ▶ Deployment Scheduling Methodology
- ▶ Notional Order of Deployments to an Agency Site
- ▶ Preparation of Agency-Specific Transformation Plans
- ▶ Order of Agencies receiving Deployment Rollouts in 1Q and 2Q 2007
- ▶ Agency Preparation

## Team Structure & Roles

- ▶ Deployment Roles & Responsibilities
- ▶ Resources needed to Support Transformation
- ▶ Agency Responsibilities to help insure Preparation & Readiness
- ▶ Oversight Mechanisms to Manage Transformation

## Next Steps

- ▶ Channels of Communication
- ▶ Where are we at so far with Transformation
- ▶ Data Center / Server Move

# Transformation Overview

## Transformation Overview

- ▶ What is Transformation?
- ▶ What does Transformation include -- what's going to be "transformed"?
- ▶ What's the end state?
- ▶ What's the benefit of Transformation?

## “Transformation” is a three year program to modernize the Commonwealth’s information technology infrastructure

- From**
- 68,000 desktops (varying standards)
  - 40+ help desks
  - 3,000+ servers
  - 85+ Internet connections
  - No common SLA management
  - Ad hoc, inconsistent processes / procedures

- To**
- **Standard platform and images**
  - **1 Enterprise Help Desk**
  - **1,000 Physical Servers (Target)**
  - **2 Redundant Internet Connections**
  - **Enterprise SLA Standards**
  - **ITIL Compliant Processes / Procedures**

### Key Elements

- Enterprise computing resources, including mainframes and servers
- Personal computing resources, including desktop and laptop computers
- Voice and data networks
- Help desk services
- Data center facilities
- Information security and disaster recovery services



**NORTHROP GRUMMAN**

### Messaging Services



Enterprise Exchange/Outlook Email  
Enterprise Collaboration tools  
Active Directory, DNS

### Desktop



Mass Desktop Refresh Projects  
Network Printer Consolidation and Refresh  
Enterprise Desktop Management Systems

### Help Desk



Enterprise Help Desk in Lebanon and Meadowville  
Field Based agents and technicians for Level 3  
Enterprise Help Desk System (Peregrine)

### Mainframe and Servers



New IBM and Unisys Mainframes in new Data Center  
Consolidation and refresh of servers  
Migration of servers to the data center

# Transformation

**Reliable, High Performance,  
Enterprise-Wide IT Infrastructure**

**“People – Process – Tools”**

### Security



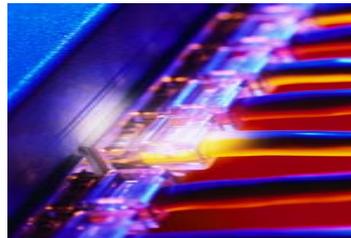
Enterprise Security Operations Center  
Computer Security Incident Respon Center  
Secure Internet Gateway

### Facilities Tier 3 and Tier 2



New Data Center/Office Building in Meadowville  
New Disaster Recovery Center and Help Desk  
in Lebanon/Russell County

### Network



New Commonwealth-wide MPLS Core WAN  
LAN upgrades to local switches/routers as needed  
Network Re-addressing of IP, DHCP

### Voice / Video



Voice over IP Network optimized for  
voice and video traffic

## Agency Benefits from Transformation

- Transformation will result in a standardized, centralized, 21<sup>st</sup> century IT environment
- At the end of three years, agencies will experience a reliable, high performance, enterprise-wide IT infrastructure
- Transformation will provide agencies with access to new technology that will help them deliver services more efficiently and effectively
- Transformation will make it possible for agencies to enhance their services to the citizens of the Commonwealth
- Transformation will help resolve or prevent IT challenges existing today and position agencies to provide enhanced capabilities in the future

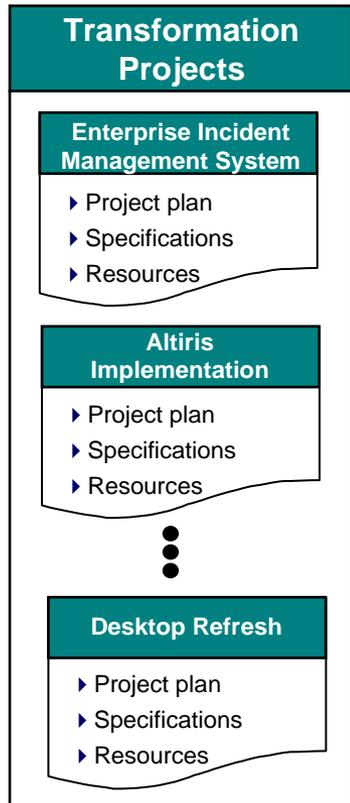
# Deployment Approach and Impacts

## Deployment Approach

- ▶ How is the rollout going to occur?
- ▶ In what order will we receive new services?
- ▶ How will my agency's unique needs be addressed?
- ▶ What can I do to make my agency's transformation successful?

# Scheduling Methodology

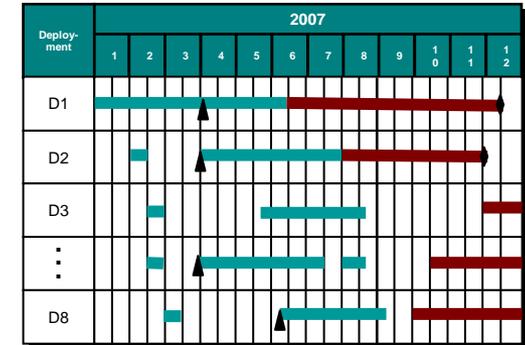
48 individual projects



... are grouped into 8 rollout deployments based on the following considerations

- ▶ Commonalities among projects (e.g., type of project, technical platform, staff required)
- ▶ Interdependencies across projects (e.g., deliverables/milestones, exchange of data)
- ▶ Required technology progression

... and scheduled to Agency sites



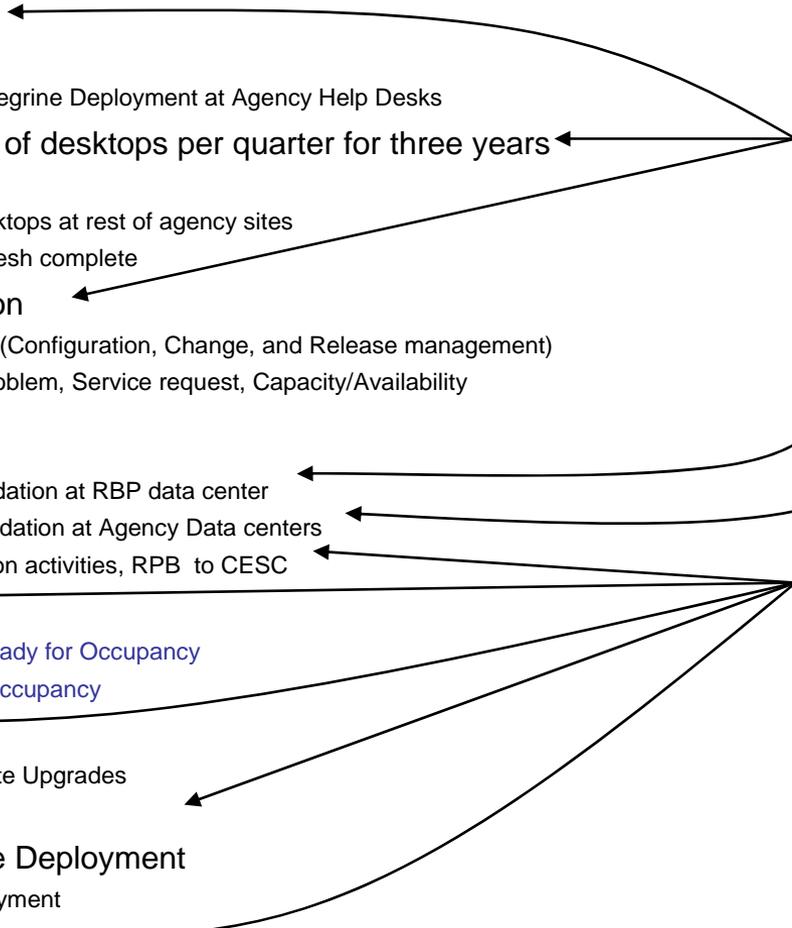
- 8 deployments x 81 agencies
- 648 schedules at that Agency level
- Thousands of schedules at the site level

## Notional Order of the 8 Transformation Deployments

- Incident Management System
  - Jan. 2007 – Pilot Sites
  - Feb. 2007 – Begin Enterprise Peregrine Deployment at Agency Help Desks
- Desktop Refresh - targets 12% of desktops per quarter for three years
  - Jan. 2007 – Pilot sites
  - Feb. 2007 – Begin refreshing desktops at rest of agency sites
  - Feb. 2009 – 90% of desktops refresh complete
- ITIL Deployment and Integration
  - April 2007 – Phase 1 deployment (Configuration, Change, and Release management)
  - Nov. 2007 – Phase 2 (Incident/Problem, Service request, Capacity/Availability Management)
- Server Consolidation
  - Feb 2007 – Begin Server Consolidation at RBP data center
  - April 2007 – Begin Server Consolidation at Agency Data centers
  - July 2007 – Begin Server relocation activities, RPB to CESC
- Data Center
  - July 2007 – CESC Data Center ready for Occupancy
  - Nov. 2007 – SWESC Ready for Occupancy
- Network
  - July 2007 - Begin Agency MAN site Upgrades
  - Remaining Site Schedule TBD
- Enterprise End User Exchange Deployment
  - Sept. 2007 – Begin Agency deployment
- Enterprise Help Desk
  - 4Q 2007 – Begin Rollout of Enterprise Help Desk

These projects can be run without dependency on our data center

These projects cannot be run without dependency on our data center



## Going from Notional Order to Agency Planning

**Notional Order of Transformation Deployments**

- Incident Management System
- Desktop Refresh
- ITIL Deployment and Integration
- Server Consolidation
- ...

**COMPLETE**

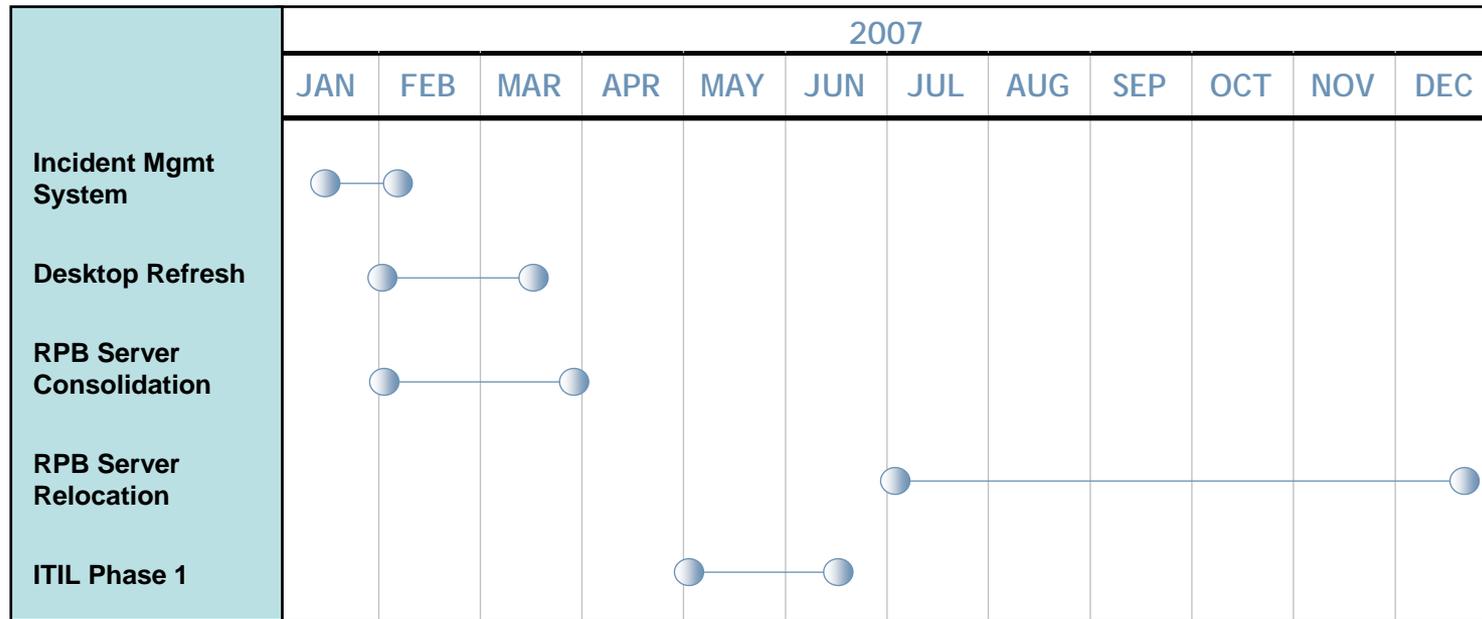
- ▶ Started with individual Transformation projects
- ▶ Grouped projects where possible, factoring in dependencies, objectives and business requirements
- ▶ Developed a Notional Order of Transformation Deployments



**IN PROGRESS**

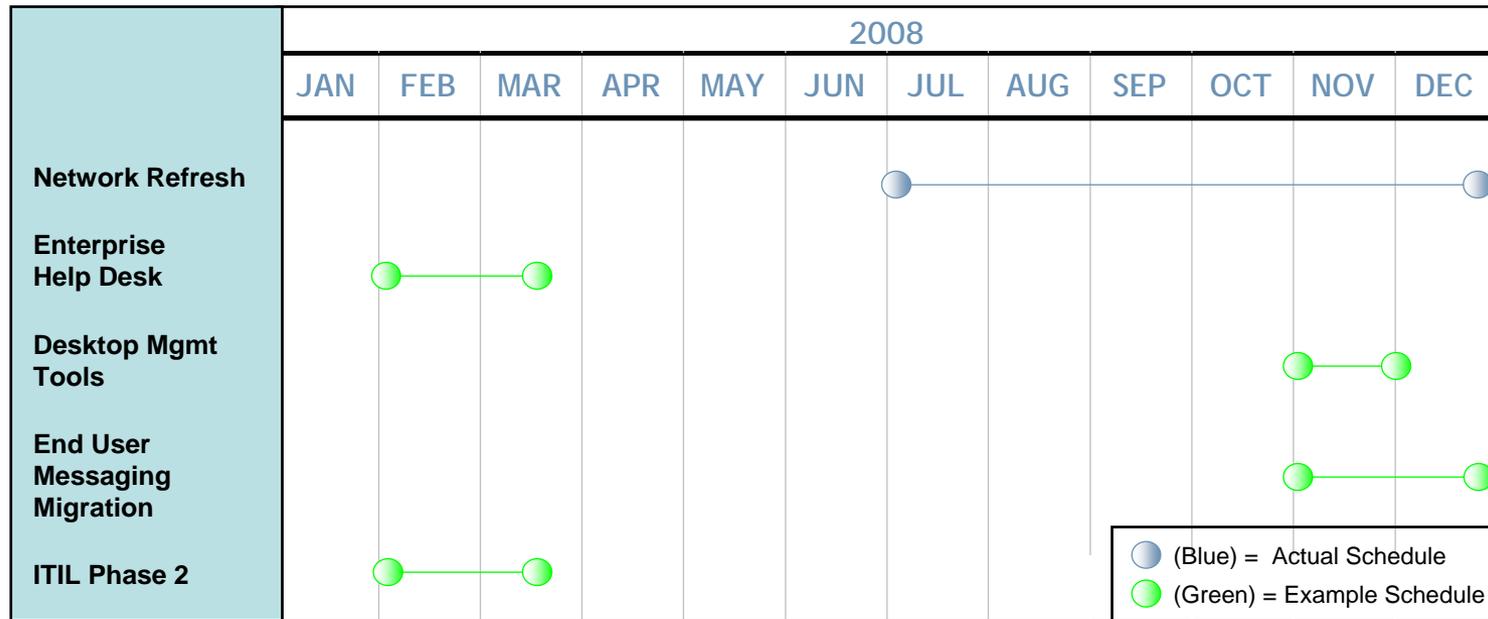
- ▶ Apply the Notional Order to Agency schedules
- ▶ Develop Agency-specific Transformation Plans

## Example Agency Transformation Plan ~ Department of Correctional Education ~



- ▶ Transformation schedules are created from the Notional Order table
- ▶ Agencies can have multiple Transformation projects running
- ▶ Dependencies on other infrastructure projects will mean Transformation projects will come in different parts of the calendar year

## Example Agency Transformation Plan ~ Department of Correctional Education ~



- ▶ As infrastructure projects complete (Data center, Core Networks, etc.) remaining Transformation projects will occur
- ▶ Every Agency will have a scheduled time for each sub-project managed through one master schedule with project plans rolled into a single Agency master plan

## Addressing Agency Unique Needs and Making Transformation a Success

- Agency participation is critical to ensuring that business requirements are met
- Transformation Project Teams will provide due diligence worksheets prior to each deployment

**EXAMPLES**

**~ Typical Areas to be Addressed by Agencies ~**

- |  |   |
|--|---|
| <ul style="list-style-type: none"> <li>▶ Identify a Transformation POC</li> <li>▶ Evaluate deployment methods</li> <li>▶ Validate applications with hardcoded IP addresses</li> <li>▶ Validate applications that run in your desktop environment</li> <li>▶ Validate applications that run in your server environment</li> </ul> | <ul style="list-style-type: none"> <li>▶ Validate site listing for agency and availability for scheduled transformation activities</li> <li>▶ Assist in communicating significant events</li> <li>▶ Identify drop ship locations for desktop refresh</li> <li>▶ Identify end user groups and how you will communicate with them</li> <li>▶ Assess training needs</li> </ul> |
|--|---|

## Managing the Change

**We'll work with you to manage the “people side” of change and make Transformation a success**

- Managing the people side of change is critical to making Transformation a success
  - *Before and during deployment...* agency awareness and participation is critical to developing the right solution and facilitating a smooth roll out
  - *After deployment...* agency employees may need to initiate new behaviors or discontinue old ones if the agency is to capture the intended value

### Issues Agencies Face

- ▶ New and unknown technology and processes
- ▶ Requirements for additional skills and expertise
- ▶ Fear of job loss (for self or others)
- ▶ Apprehension over new Commonwealth colleagues
- ▶ Loss of decision authority or control
- ▶ Change in work location
- ▶ New expectations from superiors and peers
- ▶ Concern about applicability of current skills



**Change Management actions help you achieve your goals**

### Transformation Goals and Objectives

- ▶ New IT service concepts
- ▶ Productivity increases
- ▶ Standardized processes and procedures
- ▶ Increased collaboration
- ▶ Enterprise-wide focus
- ▶ Etc.

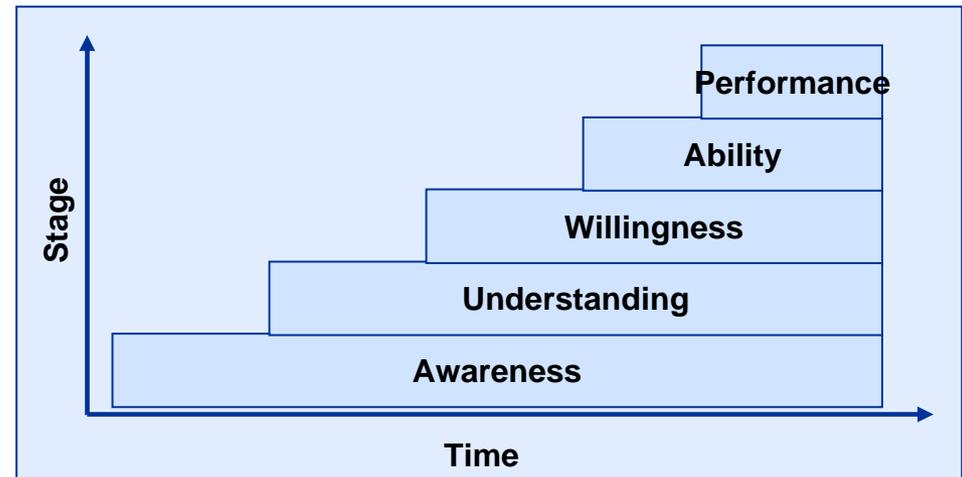
## Change Management Initiatives

### Change management is embedded throughout our deployment approach

Our deployment approach includes multiple techniques to assist agencies and their people in adopting the changes that result from Transformation and achieving the desired performance

- **Joint Deployment Team** – (customer agency and VITA) and clearly defined roles & responsibilities for deployment activities
- **Pilot roll-outs** - capture of lessons learned, and integration of those lessons into future roll-outs
- **Demonstrations** - of new software and hardware at select agency locations
- **Outreach** - to agency users through newsletters, web sites, e-mail, and “road shows”
- **Tactical tools** - such as FAQs, talking points, and toolkits to assist deployment teams
- **Networking** - Implementation of “super users” networks and communities of interest (COINs)
- **Feedback channels** - such as quick-response surveys and the questions mailbox

Stages of Change Adoption



## Team Structure and Roles

### Team Structure & Roles

- ▶ Who will manage the rollout at our sites?
- ▶ How are you going to work with us during rollout?
- ▶ What resources will be required of my agency to support the Transformation?
- ▶ How should we prepare? What do we need to do to be ready?
- ▶ What oversight mechanisms are in place to manage Transformation?

## Deployment Roles & Responsibilities

### Agency Location

#### Agency Transformation POC

- Be a Champion for Change
- Track status and work being performed along with the VITA Transformation POC
- Serve as the conduit for work and communication into their respective agency
- Perform oversight of requests within their agency

#### VITA Transformation POC

- Serve as an interface for the designated Agency POC in regards to Transformation
- Manage rollout at agency sites
- Ensure that agency-specific process and procedures are integrated into deployments

### VITA Location

#### Transformation Project Managers

- Run and manage individual project deployments
- Serve as the interface into technical teams
- Create WBS for work to be performed
- Report status to VITA Transformation POC

#### Transformation Tower Leads

- Own all sub-projects within their Tower
- Have Transformation Project Managers assigned to sub-projects in their tower
- Lead and manage architecture and teams in their towers

#### Site Deployment & Schedule Program Mgr

- Manage schedules at a program level
- Manage the VITA Transformation POC's
- Track progress and status across all Agencies

Blue

= Agency person

Gray

= VITA person

## Resources Needed to Support Transformation

- Agency Transformation POC as a “Champion of Change”
- Agency management for Communications, Oversight and “Change Awareness”
- Agency staff to support and participate in:
  - Application specific testing
  - Change approvals
  - Process / Procedure Mapping and Deployments
  - Agency Training for new Tools, Process and Procedures
- VITA partnership resources (Desk-side, Server, Network, etc.)
  - Infrastructure Validation
  - Testing
  - Change approval
  - Process / Procedure Mapping and Deployments

Support, participation, and awareness  
position agency staff to operate effectively in the transformed environment

## Agency Responsibilities to Help Ensure Preparation & Readiness

- Validate pre-deployment due diligence worksheets to ensure proper planning and deployment methodologies specific to your agency
- Coordinate proposed schedules and resources considering
  - Business operations specific to your agency
  - Access to controlled areas, escorts
  - Logistics, seating, badge access, storage areas
  - Internal IT initiatives, deployments
  - Holidays
- Engage in the Transformation process
- Ask questions

## Next Steps

### Next Steps

- ▶ Channels for Communication
- ▶ Where are we at so far with Transformation
- ▶ Data Center / Server Move

## Channels for Information

**We'll continue to leverage multiple channels to share information about Transformation:**

- Monthly AITR meetings
- Partnership Advisory Council (PAC) meetings
- Customer Account Management (CAM)
- VITA Transformation POC
- Community of Interest (COIN) meetings
- Cabinet Technology Team (CATT) meetings
- Quarterly IT Investment Board (ITIB) meetings
- Monthly ITIB Customer Advisory Council (CAC) meetings
- VITA ITP web site
- Monthly "Network News" newsletter

# Where we are so far with Transformation

- Current rollout activities are centered around:
  - **Desktop Refresh**

Completed	Started
– DVS	- DCJS Pilot
– DMBE	- Council on Human Rights
– VMNH	- DCG
– EDR	- DBA
– VMFA	- DGIF            -DEDR
  - **Incident Management (Peregrine)**
    - Deployed to VCCC
    - DMHMRSAS in close out
  - **Network Refresh**
    - Pilot Starts in June/July
    - Refresh starting with DJJ, DPB, VDOT and DRS sites and ABC stores
  - **Server and MF**
    - Consolidation work in progress at RPB
    - Agency briefings being scheduled for Consolidation
    - Mainframe Testing and Server Moves begin in August
  - **Messaging**
    - Begins 1<sup>st</sup> site at VHD in July
    - Completed VDA
  - **ITIL**
    - Change Training for Current Operations and Transformation underway
    - VITA Pilot underway

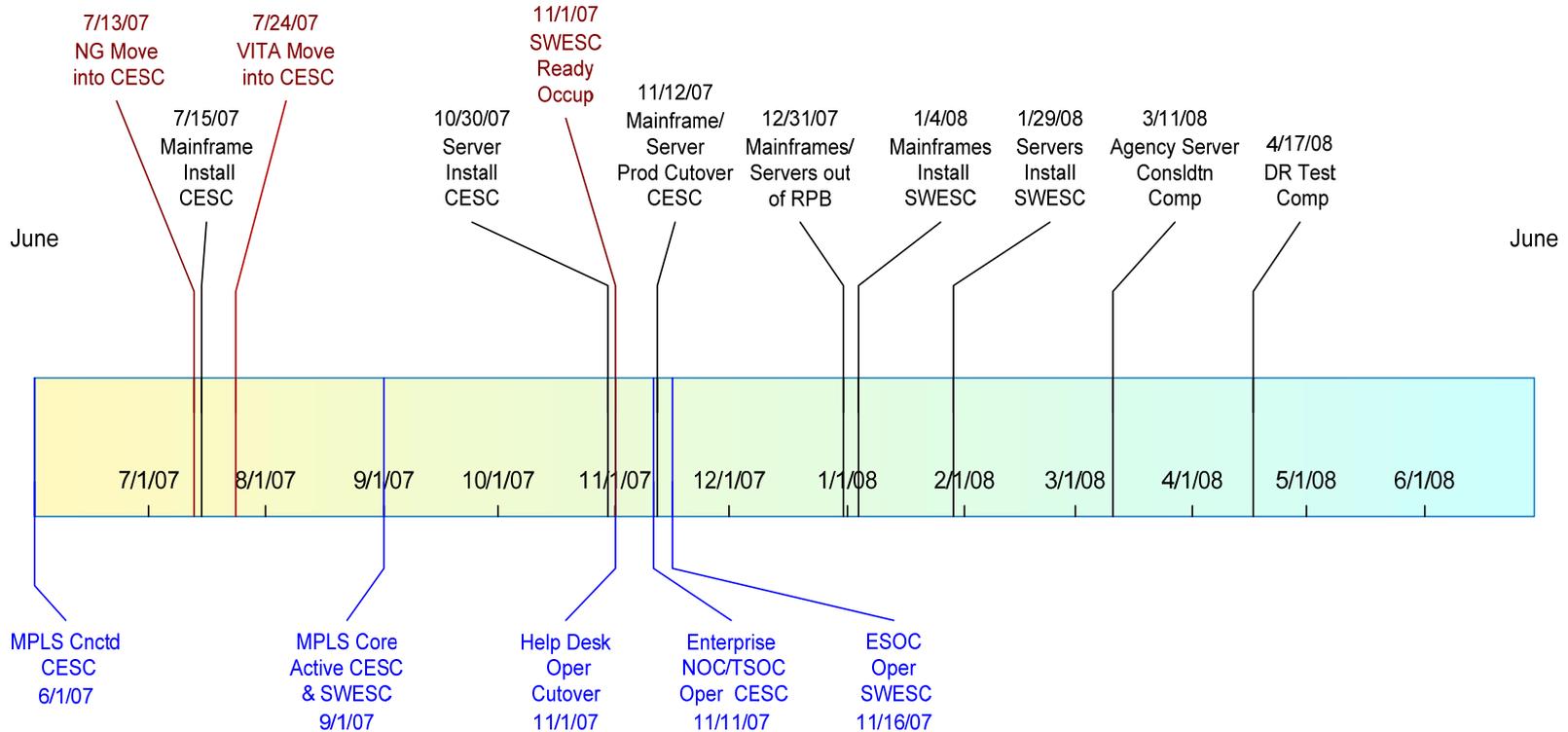
# Transformation Deployed to Operations

- Desktops (5000+ deployed)
  - Standard platform with Anti Virus and Firewall security
  - Reduces support calls required for older equipment
- Global Address List
  - Provided a single global address list for the Commonwealth of VA reducing support calls
- Peregrine live at 7 sites (14 waiting Agency Sign Off)
  - Allows for centralized ticket reporting to support teams
  - Easier metrics consolidation and monitoring
- Server consolidation
  - Standardizing Hardware platforms and added redundancy to the architecture allows for less problem outages.
- Disk Consolidation – storage
  - Removes older Hardware from the architecture.
  - Allows rapid deployment of new storage requirements
  - Allows for data replication to increase recovery timeframes
- Piloted ITIL
  - Integrated change management to increase successful change and coordination for infrastructure teams
- Network MPLS Points of presence
  - Provides redundancy for main core infrastructure.
  - Less down time and allows for maintained to be preformed while keeping network available

# Service Catalog

- **When**
  - Initial production phase start: November 15, 2007
- **Benefit**
  - Ability for End User to select “pre-packaged” bundles for quick order
  - Allows standardization across the Commonwealth
  - Easy approval process
  - For common systems “extra” and “additional” features easily identified and selected
- **Impact**
  - End user training for a new order process
  - Agency mapping for approval process
  - Custom orders still may require current P2P
  - Possible FW changes to allow access to web base tool

# Data Center Move



- Moving the data center from RPB to new, secure CESC facility is complex
  - Significant coordination with agencies, minimizing business disruptions, technical complexity
- Robust, detailed data center move plan in place
  - Move strategy, test objectives, risk mitigation, communication plan with agencies

# Data Center Move Strategy

- **Mainframe Move Strategy**

- Replicated mainframe and related hardware required for full application testing
- Coordinate all mainframe users (15 agencies)
- Provide agencies isolated external connectivity to CESC test environment
- Test environment available for 60-90 days
- Multiple mock cutover test prior to final go-live

- **Server Move Strategy**

- Virtualize/consolidate servers at RPB
- Consolidate multiple SAN/DISK storage systems at RPB
- Replicate RPB internal network (LAN) at CESC
- A two-phased cutover approach will be utilized
  - Phase 1 is movement of servers onto an extended duplicate RPB network at CESC
  - Phase 2 will require that servers be moved from duplicate RPB network to “New” network at CESC
- Servers will be moved in 7 logical groups, based primarily on agency usage

# Transformation Status

---



NORTHROP GRUMMAN

# Transformation – Current Rollout Focus

## – Desktop Refresh

### • Completed

- DVS      - DCG      - DEDR
- DMBE    - Council on Human Rights
- VMNH    - DCJS Pilot   - DBA
- EDR      - VMFA      DGIF

### Started

- DOC      -VDH      -DMHMRSAS
- DCE      -SBE
- DJJ      -VITA
- VSDBS    - Gunston Hall

## – Incident Management (Peregrine)

- Added 9 more agencies as complete

## – Network Refresh

- Pilot Starts in June/July
- Refresh starting with DJJ, VDOT and DRS sites and ABC stores
- Starting DEQ and VDH in August

## – Server and MF

- Consolidation work in progress at RPB
- Agency moves to CESC underway
- Mainframe Testing begins in August – Delayed to Sept.

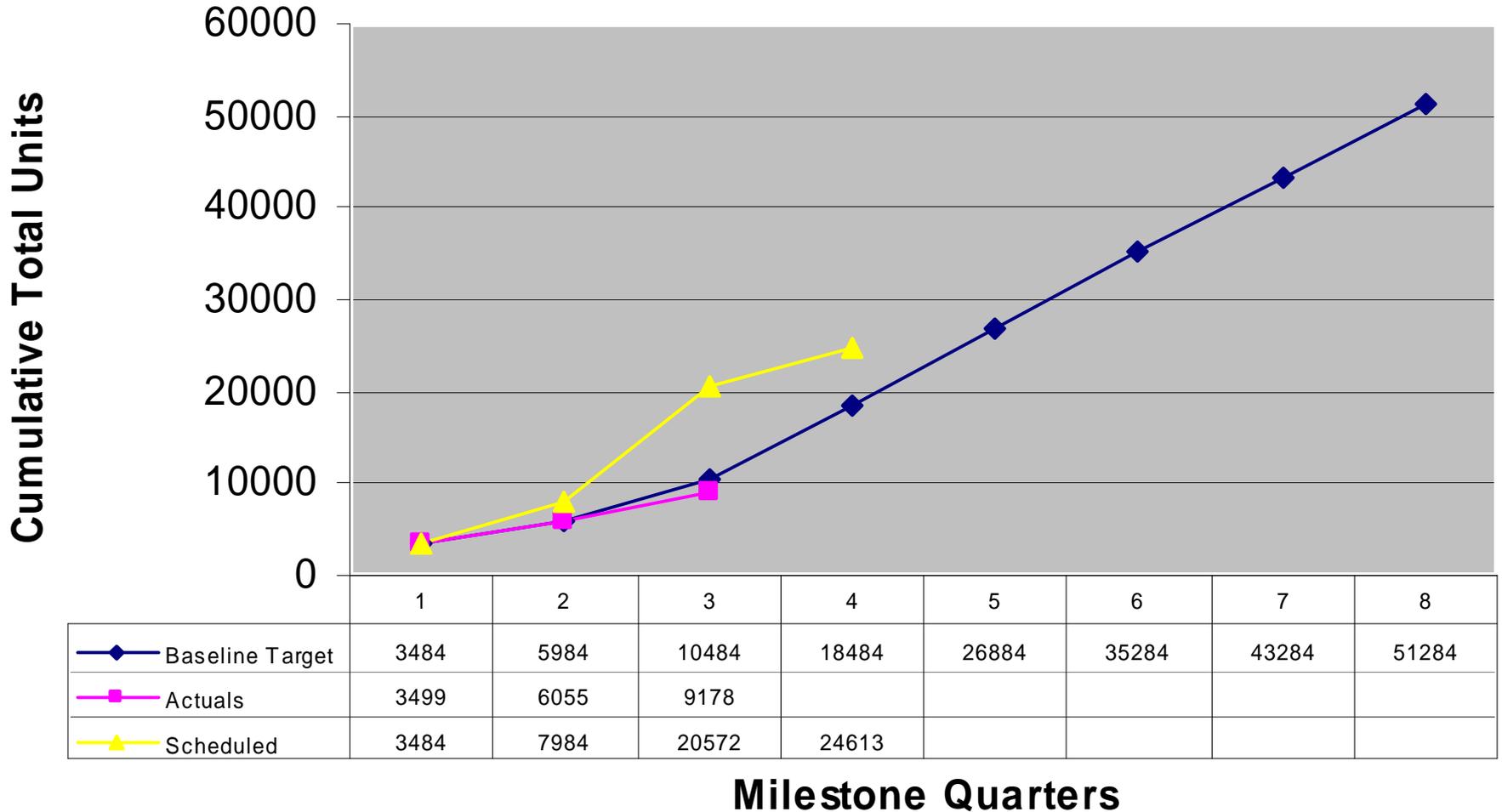
## – Messaging

- Begin 1<sup>st</sup> site at VHD in July – Begins Sept/Oct
- Completed VDA

## – ITIL

- VITA Pilot underway

## Desktop Refresh Plan



\* Data as of 8/21/07



NORTHROP GRUMMAN

# Server

**Phase 1: RPB**

 5/15/07  
Completed

**Phase 2: Greater Richmond**

8/08

**Phase 3: Enterprise**

6/09

## ✓ Phase One (RPB):

- ✓ Delayed start of Server consolidation
- ✓ Developed standards
  - Proof of tools
  - Process & Procedures
  - Team execution

## • Phase Two Greater Richmond:

- Leverage process & tools used at RPB
- Consolidate 83 RPB servers removed from the unconsolidated list
- Planned server discovery and consolidation – (near-term)
  - VDOT – 200+ servers (TAB Approved) Need to engage Agency
  - DMV - 200+ servers (TAB Approved) Completed Agency Initial Meeting 8/20/07
  - TAX - ~61 servers (TAB Approved) Need to present solution

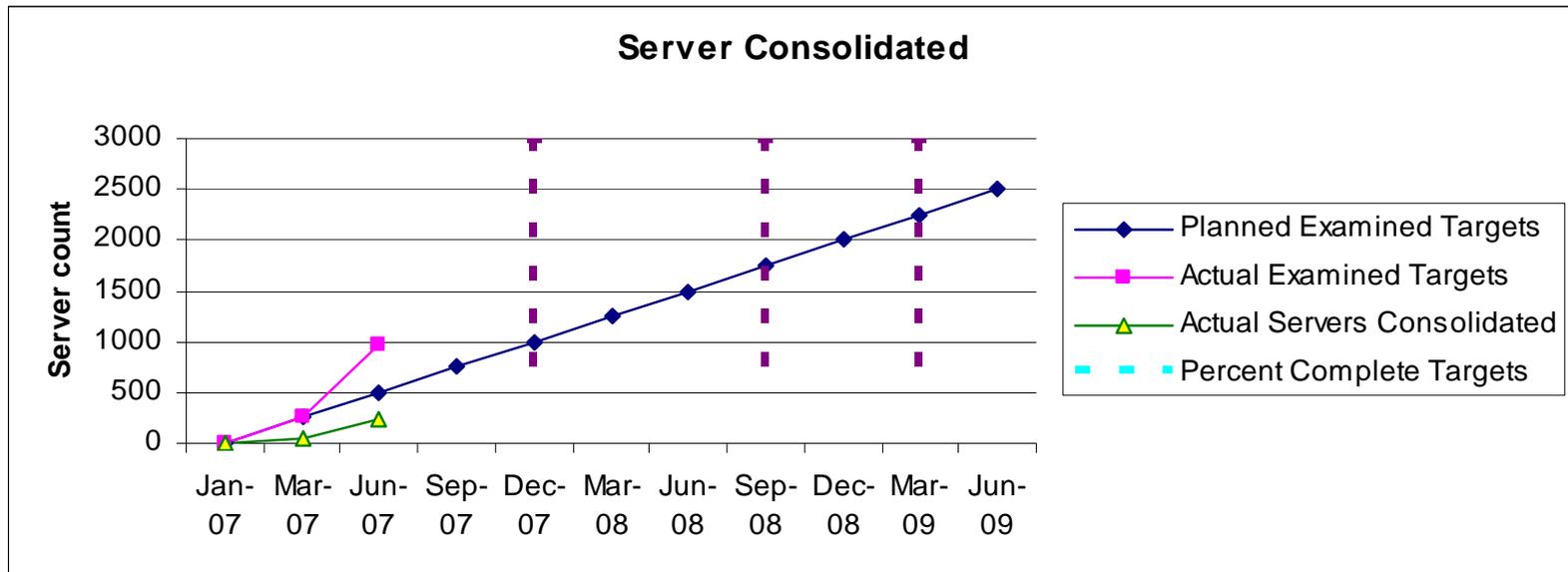
## • Server move – RPB to CESC

- ✓ Move Group 1 Complete
- ✓ Move Group 2 Complete
- On Schedule for “Move Group 3” 25 Aug date
- Project status will remain Yellow until move underway against plan
  - ✓ Project mgmt strengthened

# Server Consolidation Metrics

Phase 2: Greater Richmond

Phase 3: Enterprise



- To-Date NG has evaluated 968 systems for consolidation (target for goal was 618 systems to be evaluated)
- Additionally 245 of 2500 systems have been consolidated to-date.

---

# Questions?



# Desktop Image/Application Security

Monty Frahm

September 13, 2007



## Agenda

- Desktop Security Aspects
- Core Image
- Agency Wide-Applications

## Desktop Security Aspects

- Standardization of PC Hardware/Software in the Commonwealth
  - Laptop
  - Desktop
  - Tablet
  
- Security Benefits
  - Reduced downtime
  - Common Layer 0, Layer 1 Image
  - Facilitate Asset Inventory Process

# Core Image

## Core Image Design

➤ *Based on CIS Benchmarks for Windows XP*

- Widely accepted by US Government Agencies
- GLBA, SOX, HIPAA, FERPA Compliant
- VITA Security Exception Process

<http://www.vita.virginia.gov/uploadedFiles/Library/ITRMSEC501-01ITSecStd.pdf>

➤ Core image for across Commonwealth

- Desktops
- Laptops
- Tablets

➤ Image Layers

- Layer 0
- Layer 1

## Core Image

### Image Design – Layer 0

- *Base Operating System*
  - *Service Packs - Windows XP SP2*
  - *Windows Security Patches*
    - *Current as of June 2007*
    - *Ongoing security patches rolled out via policy (8 PM each night) to Windows Update or WSUS if agency has that service*
    - *Firewall Settings – Policy Controlled*
- *“Clean machine” for packaging to avoid capturing application dependencies.*
- *Will not be deployed to End User desktops*
- *Used by packaging team to build application packages*
- *Base for Layer 1 Image*

# Core Image

## Image Design – Layer 1

- Core Commonwealth image
  - Desktops
  - Laptops
  - Tablets
  
- Commonwealth Wide-Applications – In use by entire Commonwealth (Layer 1 Applications)
  
- Contains
  - Layer 0 Image
  - Layer 1 Applications
  - Altiris Client

# Core Layer 1 Applications

Application Name	Version
Adobe Reader	7.0.8
Flash Player	9
Shockwave Player	10
Altiris Agent	6.8.206
Quicktime Viewer	7.1
Authorware Player	7
VirusScan Enterprise	8
AntiSpyware Enterprise Module	8
.NET Framework	1.1
Powerpoint Viewer	2003
Visio Viewer	2003
Windows Installer	3.1
Windows Media Player	10
Windows Messenger	5.1 (shortcut disabled by local policy)
Visual Basic Runtime	6.0 SP5
Real Player	10
WinDVD for HP	6.2
Roxio Suite including DVDPlus, Audio, Data, Copy, Labeler and LiteScript installed depending on hardware	2.0.4
Orientation Guides	1

# Core Layer 1 Application Security

## Examples

- MS Office 2003 Security Settings
  - Agency Defined in load set
  
- IE Security Settings
  - Set Default Homepage to <http://www.state.va.us>
  - All other settings are default
  
- McAfee Security
  - Update via web (McAfee)
  - Agency Defined in load set
  
- MS Messenger 5.1
  - Shortcut disabled by local policy
  
- All others contain Default or Agency defined settings

## What's next?

### Agency-wide applications

- Layer 1 Image plus Agency Load set - Software
  
- Contains
  - Layer 0 Image
  - Layer 1 Applications
  - Altiris Client
  - Software Utilized by entire Agency

# Questions

?



# Desktop Image/Application Security: VAR Approval Process

Todd Kissam  
September 13, 2007



**NORTHROP GRUMMAN**

## What is VAR?

### VITA Architecture Review

All VITA operations centers hosted services that are being changed, developed or procured that will change the VITA Enterprise IT Infrastructure require approval prior to implementation or procurement.

This approval process is governed by the Commonwealth Policies, Standards, and Guidelines (PSG) for Enterprise Architecture and Security Architecture best practices.

## Who reviews?

- ▶ ITIES: PPA Director
- ▶ Northrop Grumman (NG): Chief Architect
- ▶ SMO: Senior Manager of Security Operations)
- ▶ SMO SDM Tower Leads
  - Help Desk Services
  - Mainframe & Server Services
  - Network and Telecommunications Services
  - Messaging Services
  - Desktop Computing Services
  - Internal Applications Services
- ▶ Architects: Enterprise, Application & Data
- ▶ Commonwealth Security & Risk Management
- ▶ Operations

## How are requests reviewed?

- ▶ By Domain (example: Data):
  - ▶ Objective Review
    - Compliance
  - ▶ Subjective Review
    - Recommended practices
    - Other
- ▶ 10 Business days

## Example: Applications

### ▶ Objective review:

- Web Application Security Development & Maintenance Policy
- Web Application Security Development & Maintenance Procedure
- Website Development Procedure
- Website/Webserver Security Policy

### ▶ Subjective review:

- Identify recommended Application designs and tools using an enterprise focus found in:
  - ETA Applications Domain Report
  - ETA Integration Domain Report

## Example: Security

### ▶ Objective review:

#### – Policies:

- Business Continuity Policy
- Customer Agency Data Protection Policy
- Customer Agency Data Protection and Recovery Procedure
- Data Center Access Policy
- Data Center Security Procedures
- Email Attachment Server Policy & Procedure
- Firewall and VPN Policy
- Information Security Incident Reporting Procedure
- Information Security Policy
- Logical System Access Control Policy and Procedure
- Password Usage Policy
- Publicly Accessible Server Administration Policy
- Publicly Accessible Server Administration Procedure
- Removal of Data from Hard Drives and Electronic Media Policy & Procedure
- Security Policy Exemption Policy & Procedure
- virginia.gov Internet Domain Naming Policy
- Web Application Security Development & Maintenance Policy
- Web Application Security Development & Maintenance Procedure
- Website Development Procedure
- Website/Webserver Security Policy

## Example: Security

### ▶ Objective review:

#### – Hardening Standards

VITA AIX Hardening Standard

VITA Apache Server Hardening Standard

VITA BIND Database Hardening Standard

VITA Checkpoint Firewall Hardening Standard

VITA CISCO PIX Firewall Hardening Standard

VITA CISCO Router Hardening Standard

VITA CISCO Switch Hardening Standard

VITA Exchange Hardening Standard

VITA FreeBSD Hardening Standard

VITA HPUX Hardening Standard

VITA IIS Hardening Standard

VITA LINUX Hardening Standard

VITA Oracle 9i Hardening Standard

VITA Oracle Database Hardening Standard

VITA Red Hat LINUX Hardening Standard

VITA SOLARIS Hardening Standard

VITA SQL Server 2000 Hardening Standard

VITA WINDOWS 2000 Server Hardening Standard

VITA WINDOWS 2003 Server Hardening Standard

VITA WINDOWS NT Hardening Standard

VITA WINDOWS XP PRO WS Hardening Standard

Security Configuration Standard Exception Process

## Example: Security

### ▶ Objective review:

- Security Architecture  
Security Architecture Report

### ▶ Subjective review:

- Security Best Practices
- Answers to the AAA of Security: Authentication, Authorization, and Accounting
- Interaction with other systems.
- Emerging strategic direction for the Commonwealth of Virginia.

# Questions

?



# Local Administrator Rights

Cathie Brown, CISM, CISSP  
Deputy Chief Information Security Officer

---

ISOAG Meeting  
9/13/2007



# Introduction

- Why do we need a presentation?
  - Review what the Standard says
  - Cover what could go wrong
- Exception process
  - Paperwork
  - Approval
- Good reasons for administrator rights
- Bad reasons for administrator rights



## Per the IT Security Standard

- Section 5 Logical Access Control
- 5.2.2 #16 Require that System Administrators have both an administrative account and at least one user account and require that administrators use their administrative accounts only when performing tasks that require administrative privileges.
- 5.2.2 #17 Require that local administrator rights, or the equivalent on non-Microsoft Windows-based IT systems, be granted only to authorized IT staff.



## Why Local Admin Rights are a Bad Idea

- Local user can change security settings
  - Disable automatic idle lockout
  - Change firewall settings
  - Modify other user accounts
- Unsupported programs can cause instability
  - Break updates that function on a standard image
  - Prevent the function of newly installed tools
  - Lock out help desk access
- User is more vulnerable to attack
  - Can modify their normal account for admin access
  - Attacks that would normally compromise the user compromise the entire system
  - System compromise more easily leads to network compromise



## Exceptions to the Standard

- ALL exceptions MUST be approved
  - Agency Head
  - VITA Commonwealth Security
- Reasons for the exception must be clear
  - Include business or technical justification
- The exception should be very specific
  - Which systems does it apply to?
  - Duration (not to exceed 1 year)?
  - What are the associated risks?
  - Can the need be addressed through other means?
  - What training has the user received that mitigates the risk?
- A second account must be used for Administrator rights



## Good Reasons for an Exception

- Needs to install and run software that MUST have Administrator Rights
- Needs frequent access to disk utilities
- Developers who need access to debugging functions
  - Frequently this access can be granted through other means
- Other functions that Require the use of Administrator privileges



## Bad Reasons for an Exception

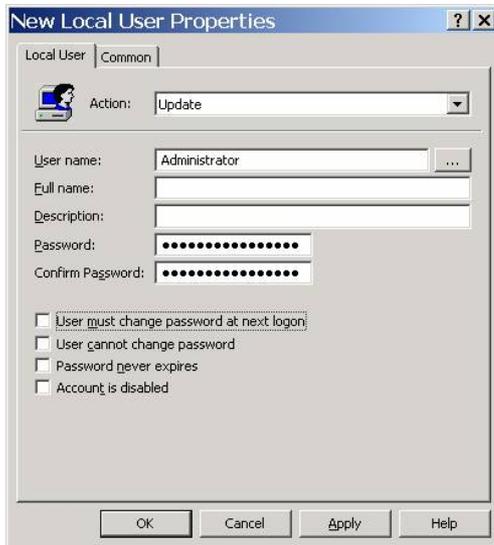
- Routinely needs to install software
  - New software needs support approval
  - In most cases can be installed by a power user
- Needs to change the IP address
  - DHCP is used throughout the Commonwealth
  - DHCP is used in 99% of homes
  - DHCP does not require Admin rights
- Travels frequently
  - Needs to change configurations to connect



## Why 2 accounts?

- Local Administrator Account to be used as necessary while performing work that requires administrative privileges
- User Account to be used at all other times such as working in email, performing research on the web, etc.
- Minimize risks associated with admin privileges

# Questions?



## Resources for reference:

- The Administrator Accounts Security Planning Guide  
[www.microsoft.com/technet/security/guidance/serve\\_rsecurity/administratoraccounts/default.mspx](http://www.microsoft.com/technet/security/guidance/serve_rsecurity/administratoraccounts/default.mspx)
- How To: Secure Your Developer Workstation  
[msdn2.microsoft.com/en-us/library/Aa302367.aspx](http://msdn2.microsoft.com/en-us/library/Aa302367.aspx)



Virginia Information Technologies Agency

# Honeypots or “How I Learned to Stop Worrying and Love the Malware”

**Tripp Sims**

Commonwealth of Virginia Security Architect

---

ISOAG

September, 2007

Questions & Comments: [tripp.sims@vita.virginia.gov](mailto:tripp.sims@vita.virginia.gov)



# Content

- Honey pots in a Nutshell
- Network Honey pots & Honey nets
  - Low Interaction vs High Interaction
- Honey clients
  - SCOUT, Capture-HPC, and deJscript
- Other Honey pot Technology
  - GHH, SMTarPit, Open Proxy, Honeytokens
- Putting it all into practice...
- Questions and Answers



# Honeypot in a Nutshell

The term honeypot, in computing terms, has varied definitions depending on the exact area of computing to which you refer.

A good generic definition is:

***“A computing resource which acts as trap to detect computer and network misuse.”***

The etymology of the word in computing terminology is generally considered to refer to the children’s character Winnie the Poo, the stuffed bear usually lured into trouble from his desire for honey.

Today we have network honeypots (high interaction & low interaction); client honeypots; spam traps; proxy traps; and finally honeytokens.



# Network Honeypots & Honeynets

Network honeypots are deployed to emulate vulnerable network services.

- **Low interaction:** honeypots consist of a program (or collection of programs) which emulate one or more vulnerable operating systems and applications. At no time is an actual vulnerable system presented to the attacker. Low interaction honeypots like nepenthes and honeyd enable one server to act like thousands of vulnerable systems, i.e.; a *honeynet*.
- **High interaction:** honeypots consist of real machines running real vulnerabilities. Typically the traffic flow to and from these machines is tightly controlled by an in-line IDS/Firewall. That advantage to high interaction is the ability to utilize native tools (Explorer, Instant Messenger, etc.) in order to glean more information about an attacker.



# Honeyclients

Unlike Honey pots which sit passively waiting to be attacked, Honeyclients are clients which are deployed to actively seek out malicious content.

Honeyclients usually require a minimum of a virtual machine in which to run. A few can emulate and fingerprint known attacks and vulnerabilities without running an entire OS - but this approach has the obvious drawback of missing unknown, or "0 day", attacks.

It is telling that almost all Honeyclient implementations currently revolve around the Internet web browser.

# SCOUT - Speedy Complete Online URL Test

## SCOUT - Speedy Complete Online URL Test

This page allows you to submit a suspicious URL to our high interaction client honeypot Capture to determine whether the suspicious URL is indeed malicious. The client honeypot, which runs Windows XP and Internet Explorer 6, will make the request to the server and determine whether any unauthorized state changes, such as placing an executable file in the start-up folder, have been made. If these state changes are detected, our client honeypot will classify the URL as malicious.



Please enter a suspicious URL (for example <http://www.google.com>).



Suspicious URL (starting with <http://>):

Security Code:

This service has been made possible by [Victoria University of Wellington](#). Because there are only limited amount of hardware resources behind this service, concurrent requests have been capped. If the page indicates that the client honeypot is busy, please try back again later. Help us to expand this service by donating. See <https://www.client-honeynet.org/donations.html> for more details on how to donate.

SCOUT is a free online service provided by Victoria University of Wellington in New Zealand.

It is a scaled out implementation of the freely available Capture-HPC framework.

In about 60 seconds any suspect website can be validated as either malicious or cleared as benign with a very low zero false-positive rate.

[1] Go to SCOUT; [2] Paste suspect URL; [3] Enter code and submit.

SCOUT URL: <https://www.client-honeynet.org/cwebservice.php>



## Capture-HPC

Capture-HPC is a high interaction honeyclient framework. It is freely available from <https://www.client-honeynet.org/creleases.html>.

The current implementation requires at least two virtual machines. A server acts as controller for the one or more clients acting as vulnerable machines. Utilizing a framework approach such as this enables the process not only to utilize a multitude of clients capable of accessing HTTP data - it also allows you to draw comparisons between varying patch levels.

Case example:

- Client 1 (XP SP1 minimum vulnerability patches installed) connects to <http://malicious.server.com/>, is exploited, and changes to the base state of the machine are documented.
- Client 2 (XP SP2 maximum vulnerability patches installed) connects to <http://malicious.server.com>, is also exploited and changes to the base state of the machine are documented.

In this case it can be deduced that the malicious server is employing a zero day attack.



# DeJscript

DeJscript is currently in development at Arbor Networks but is unfortunately not available for general release yet. It is worth mentioning however, as it represents an impressive ability to decode obfuscated Javascript and more recently VBScript which are used to attack the browser.

## JScript Extracting Tool

**Extracted URLs:**

```
http://www.cordon.ru/mp//anifile.php
V style = "CURSOR: url('http://www.cordon.ru/mp//anifile.php')" >< /DIV >< /DIV >
var urlRealExe = 'http://www.cordon.ru/mp//file.php';
```

**Exploits used:**

**Tool**

	Exploited software	CVE ID
	Microsoft.DbgClr.DTE.8.0	<a href="#">CVE-NOMATCH</a>
	MDAC MS06-014	<a href="#">CVE-2006-0003</a>
Decode t	SoftwareDistribution.WebControl.1	<a href="#">CVE-NOMATCH</a>
	http://vMicrosoft.WMIScriptUtils.WMIObjectBroker	<a href="#">CVE-2006-4704</a>
User-Ag	Outlook.Data.Object	<a href="#">CVE-NOMATCH</a>
	DExplore.AppObj.8.0	<a href="#">CVE-NOMATCH</a>
Scan res	Business.Object.Factory	<a href="#">CVE-NOMATCH</a>
	WinZip	<a href="#">CVE-2006-5198</a>
	RDS.Dataspace MS06-014	<a href="#">CVE-2006-0003</a>
	QuickTime	<a href="#">CVE-2007-0015</a>
	VsaIDE.DTE	<a href="#">CVE-NOMATCH</a>
	VisualStudio.DTE.8.0	<a href="#">CVE-NOMATCH</a>
	Outlook.Application	<a href="#">CVE-NOMATCH</a>
	SoftwareDistribution.MicrosoftUpdateWebControl.1	<a href="#">CVE-NOMATCH</a>
	VsmIDE.DTE	<a href="#">CVE-NOMATCH</a>

# Other Honeygot Technologies

- GHH - The Google Hack Honeygot
  - Differentiates itself by emulating “known vulnerable” Web applications and using Google indexed web pages you are hosting to give hackers a window to attack your “vulnerable” applications.
- SMTarPit - An email Honeygot and Tarpit
  - When used in conjunction with honeytokent email addresses which are seeded on pages which get indexed by major search engines, SMTarPit can prove to be both an effective Honeygot or Tarpit against SPAM and malware.
- Open Proxy - ProxyPot and Open Proxy Honeygot
  - Open Proxies are utilized by purveyors of spam, as an IP anonymizer for hackers and other nefarious purposes. ProxyPot and the Open Proxy Honeygot are methods to monitor and block those attempting to utilize open proxies.



# Other Honeytrap Technologies

- Honeytokens - Trackable Data
  - Honeytokens essentially represent any unique data for which you can track the utilization of. Tokens used in the past have included fake, but operational, email addresses; login credentials for fake applications; fake credit card and personally identifiable information stored in databases.



# Putting it into practice...

The most common question that revolves around honeypot technologies is, *“What value do I gain from running a honeypot?”*

## Network Honeypots & Honeynets

- Offer a virtually zero false positive rate methodology for identifying malicious traffic destined to your network.
- Strategically positioned Honeynets on both the Internet border and LAN border of your network can operate as both early warning systems and hacker frustrators.

## Client Honeypots

- Give you the ability to evaluate the safety of a website or network resource without jeopardizing any production infrastructure.

## Honeytokens

- In scenarios where you deal with data that has a high value to a large audience it can pay hugely to develop a set of honeypot applications wherein your honeytokens can reside and be tracked when the application is breached.



# Questions and Answers

# Questions?



## UPCOMING EVENTS!

### **ISO Orientation 9/24**

9:00 a.m. -11:00 a.m. @ the Commonwealth Enterprise Solution Center

To attend please email [VITASecurityServices@VITA.Virginia.Gov](mailto:VITASecurityServices@VITA.Virginia.Gov)

Driving Directions are at

<http://www.vita.virginia.gov/uploadedFiles/ITIB/CESCDrivingDirections.pdf>

### **National State Auditors Association's IT Workshop &**

**Conference! 9/26 – 9/28** Topics include data capture & analysis in support of performance audits, auditing large & complex IT projects, information security, computer forensics, keyloggers, COBIT, cryptography & much more. The workshop will focus on auditing firewalls. For more conference information go

to: [http://www.nasact.org/conferences/conferenceinfo/IT\\_07\\_geninfo.htm](http://www.nasact.org/conferences/conferenceinfo/IT_07_geninfo.htm)



## UPCOMING EVENTS!

### **AITR Meeting 10/12**

CESEC 8:30 a.m - 11:30 a.m.

### **Virginia Alliance for Security Computing and Networking (VA SCAN) 10/18 – 10/19**

Fourth annual conference at Virginia Commonwealth University. Opportunity to hear leaders in the higher education & K-12 security field discuss current issues & share ideas on effective security practices with colleagues. Registration is \$100. Pre-registration is required. In addition to the conference program, the fee includes lunches & breaks for both days & a Thursday evening reception. To obtain more detailed see the attached conference information and to register, see <http://vascan.org>.



# UPCOMING EVENTS!

## ISOAG October Meeting 10/23

1:00 p.m. - 4:00 p.m. @ the Commonwealth Enterprise Solution Center. Driving Directions are at

<http://www.vita.virginia.gov/uploadedFiles/ITIB/CESCDrivingDirections.pdf>

### Draft Agenda:

- |   |   |
|---|---|
| Computer Crimes Unit -                          | Gene Fishel, Office of the Attorney General |
| Computer Evidence Recovery Unit Part II -       | Richard Seweryniak, Virginia State Police   |
| Managing Electronic Records as Public Records - | Ariel Billmeier, Library of Virginia        |
| IT Security Guidelines -                        | Cathie Brown, VITA                          |
| IT Security Audits -                            | TBD VITA                                    |
| Recursive DNS, The Storm Worm, and You          | Tripp Sims, VITA                            |

To attend please email [VITASecurityServices@VITA.Virginia.Gov](mailto:VITASecurityServices@VITA.Virginia.Gov)



# Any Other Business ?

---





**ADJOURN**

**THANK YOU FOR YOUR  
TIME AND THOUGHTS**

**!!!**