



Virginia Information Technologies Agency

# Commonwealth Information Security Advisory Group (ISOAG) Meeting

September 20, 2006

expect the best



# ISOAG September 2006 Agenda

- |                                    |                       |
|------------------------------------|-----------------------|
| I. Welcome & Deputy CISO Intro     | Peggy Ward, VITA      |
| II. COOP Planning                  | Brittany Schaal, VDEM |
| III. Agencies Preparedness Efforts | Curtis Brown, OCP     |
| IV. VITA COOP Planning             | Barbara Vaughan, VITA |
| V. Disaster Recovery Planning      | Dana Taylor, NG       |
| VI. Partnership Update             | Fred Duball, VITA     |
| VII. Partnership Audits            | Peggy Ward, VITA      |
| VIII. Protecting Sensitive Data    | Cathie Brown, VITA    |
| IX. Other Business                 | Peggy Ward, VITA      |



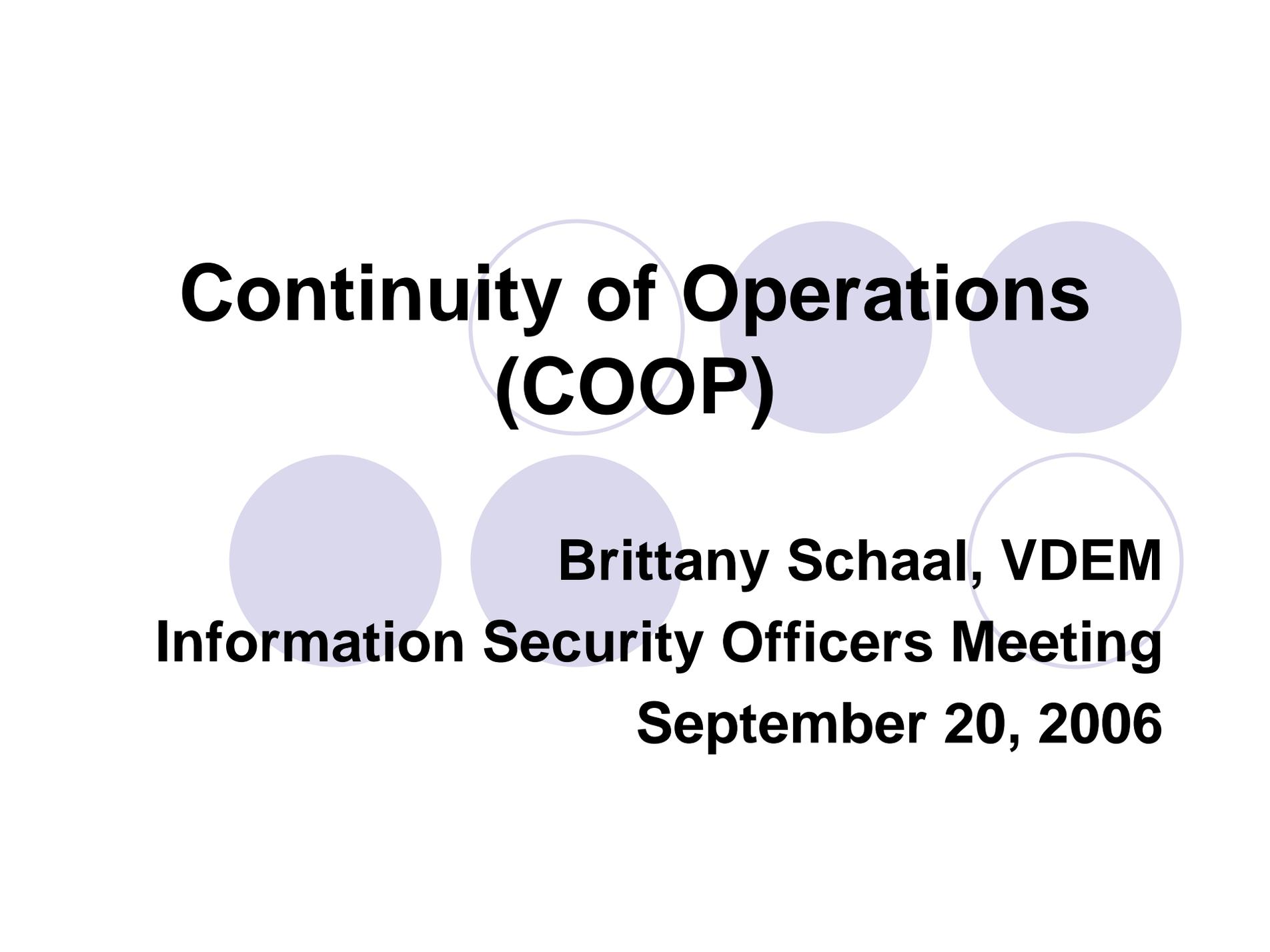
# Welcome & Deputy CISO

Welcome to each of You and Thanks for Coming!!!

Deputy Chief Information Security Officer  
Cathie Brown

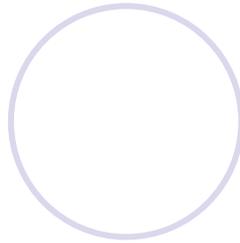
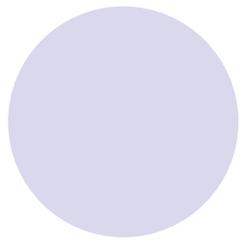
- 18 years in Healthcare IT with Centra Health in Lynchburg
- Held positions in systems programming, servers, networks and most recently Manager, Information Security & Business Continuity
- Lead HIPAA compliance efforts for Transactions & Code Sets and Security Rules, participated on team for Privacy Rule compliance
- Established Information Security Program including P&P, Security Awareness, BIA, and Auditing for Security Compliance
- Served on Joint Commission of Accreditation of Healthcare Organizations (JCAHO) Team Leaders, Safety and Security Committee, and Chair of the Information Security Committee
- Holds AAS in Data Processing from CVCC, BA in Business Administration from Averett University, and CISSP Certification



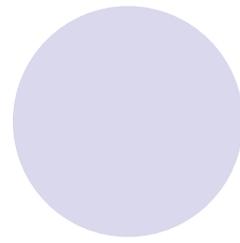
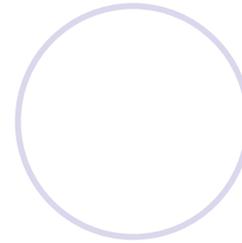
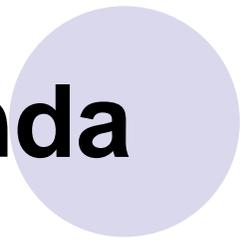


# **Continuity of Operations (COOP)**

**Brittany Schaal, VDEM**  
**Information Security Officers Meeting**  
**September 20, 2006**



# Agenda



- What is COOP?
- 10 Critical Elements
- Phases of Plan Development
- State COOP Program



# Emergency Planning: A National Security Priority

“Our cities must have clear and up-to-date plans for responding to natural disasters, disease outbreaks, or terrorist attack ... for evacuating large numbers of people in an emergency ... and for providing the food, water, and security they would need.”

“I consider detailed emergency planning to be a national security priority.”

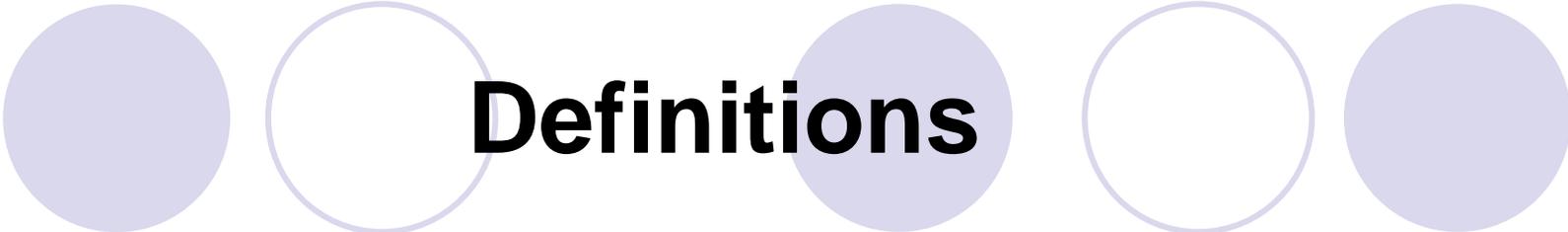
President Bush

New Orleans, September 15, 2005



# Potential Threats

<b>Natural</b>	<b>Both</b>	<b>Man-Made</b>
<p data-bbox="209 564 542 913">Ice Storm Severe Winds Tornado Hurricane Earthquake</p>	<p data-bbox="847 564 1047 763">Flood Fire Disease</p>	<p data-bbox="1285 564 1761 1063">Internet Virus Cyber Attack Agro-terrorism Chemical Explosion Water Poisoning Radiological Bio-Terrorism</p>



# Definitions

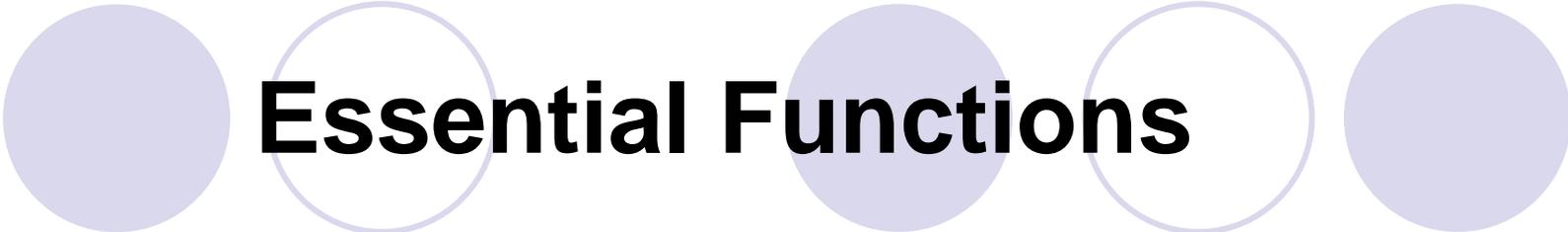
- **Business Continuity Planning (BCP)**: The effort to provide procedures to resume or restore critical business processes following a disruption.
- **Continuity of Operations Planning (COOP)**: The effort to assure that the capability exists to continue essential agency functions across a wide range of potential emergencies. Essentially, the process of maintaining the business of government.
- **Continuity of Government (COG)**: Preservation of the institution of government. Maintaining leadership, through succession of leadership, delegation of authority and active command and control. The lack of leadership can lead to anarchy or unlawful assumption of leadership.

# COOP Planning Objectives:

- Ensure the continuous performance of an agency's essential functions during an emergency.
- Ensure the safety of employees.
- Protect essential equipment, records and other assets.
- Reduce disruptions to operations.
- Minimize damage and losses.
- Achieve an orderly recovery from emergency operations.
- Identify relocation sites and ensure operational and managerial requirements are met before an emergency occurs.

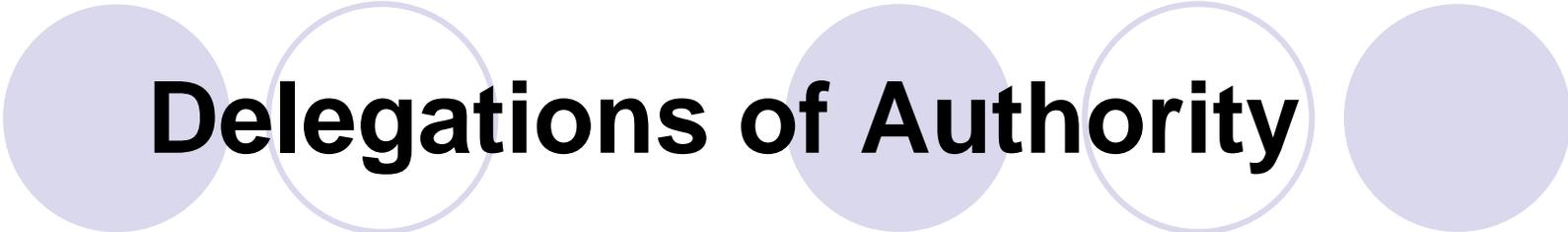
# Critical Elements of a viable COOP Plan

- Essential Functions
- Delegations of Authority
- Orders of Succession
- Alternate Facilities
- Interoperable Communications
- Vital Records
- Human Capital Management
- Tests, Training and Exercises
- Devolution
- Reconstitution



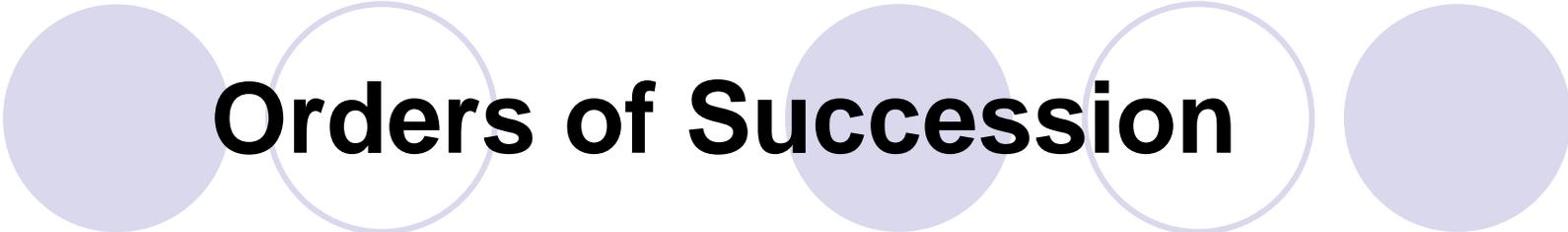
# Essential Functions

- Those functions that enable an organization to provide vital services, exercise civil authority, maintain the safety of the general public and sustain the industrial and economic base.
- Based on the agency's customers and needs.
- The foundation for COOP programs and plans.



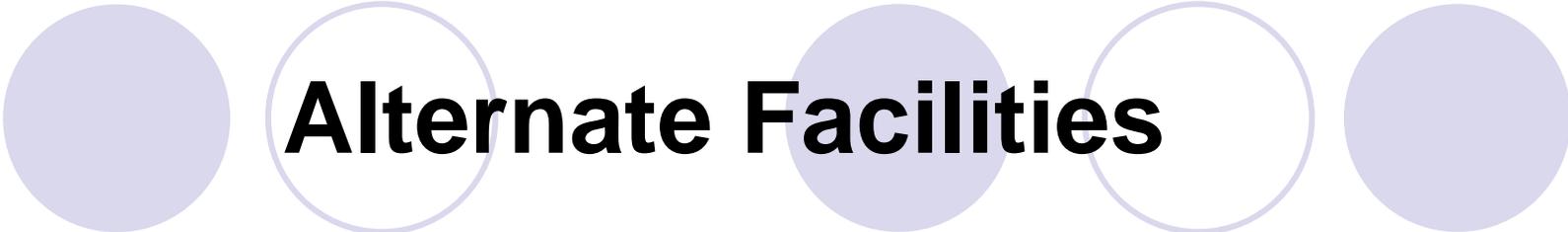
# Delegations of Authority

- Who is authorized to make decisions or act on behalf of the department or agency head and other key individuals.



# Orders of Succession

- Provisions for the assumption of senior agency leadership positions during an emergency when the incumbents are unable or unavailable to execute their duties.
- Not limited solely to management positions.

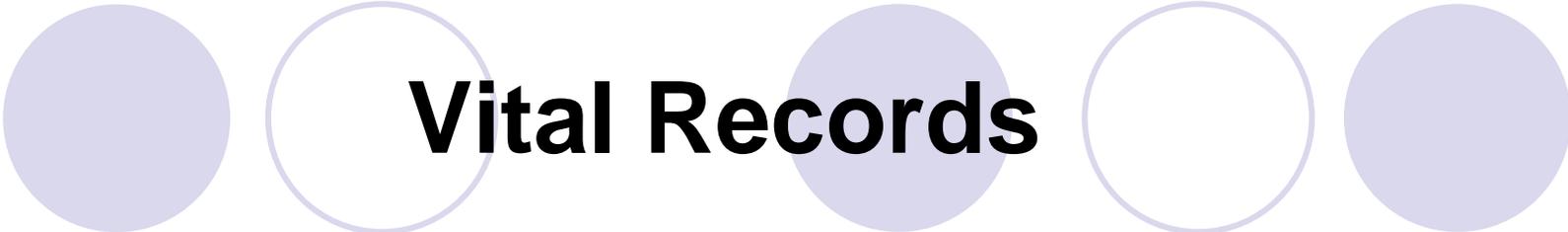


# Alternate Facilities

- A location, other than the normal facility, used to conduct critical functions/and or process data in the event that access to the primary facility is denied or the primary facility is damaged.
- The alternate site provides the capability to perform minimum essential functions until normal operations can be resumed.

# Interoperable Communications

- Provide the capability to perform essential functions, in conjunction with other agencies and organizations, until normal operations can resume.
- Interoperability is the ability of a system or a product to work with other systems or products without special effort on the part of the user.



# Vital Records

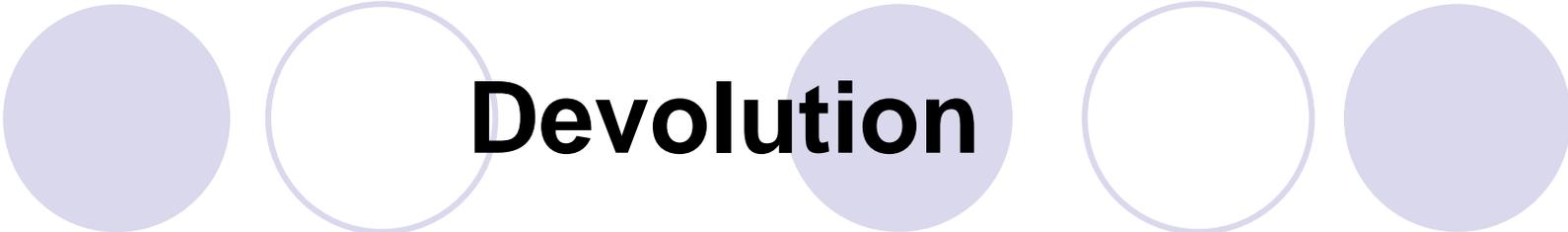
- Records that regardless of media, if damaged or destroyed would disrupt organization operations and information flow, cause considerable inconvenience and require replacement or recreation at a substantial expense.
- A system or piece of equipment is critical if it is essential to emergency operations and/or to the continuance of critical processes and services during a crisis for a minimum of fourteen days.

# Human Capital Management

- The process of acquiring, optimizing and retaining the best talent by implementing processes and systems matched to the organization's underlying mission.
- Critical in ensuring the flexibility required of key personnel during these times of crisis.

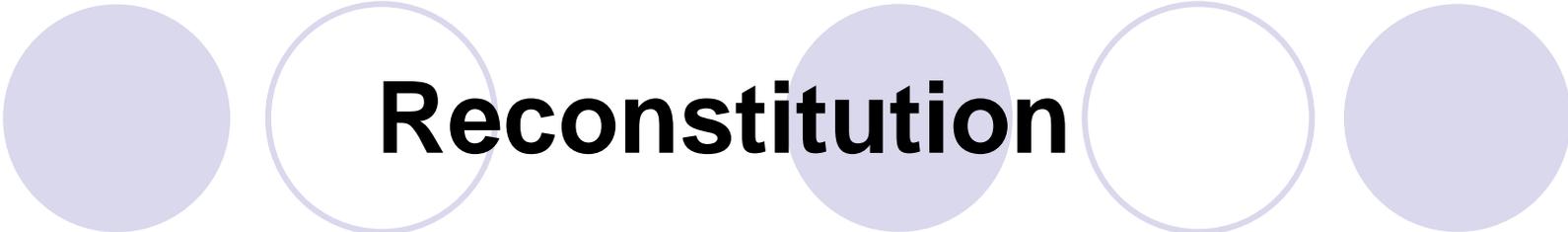
# Tests, Training and Exercises

- All staff must be educated on their role in COOP plan execution.
- Back-up systems and processes must be tested for effectiveness.
- Exercises that simulate various disruptions and practice COOP plan execution must be conducted.



# Devolution

- The capability to transfer statutory authority and responsibility for essential functions from an agency's primary operating staff and facilities to other employees and facilities.
- It is also the ability to sustain that operational capability for an extended period.



# Reconstitution

- The process by which agency personnel resume normal agency operations from the original or a replacement primary facility.
- Conducted after the emergency or disruption ceases and is unlikely to resume.

# Phases of COOP Development

- Project Initiation
- Identification of Functional Requirements
- Design and Development
- Implementation
- Training, Testing and Exercises
- Execution
- Revision and Updating



# Project Initiation

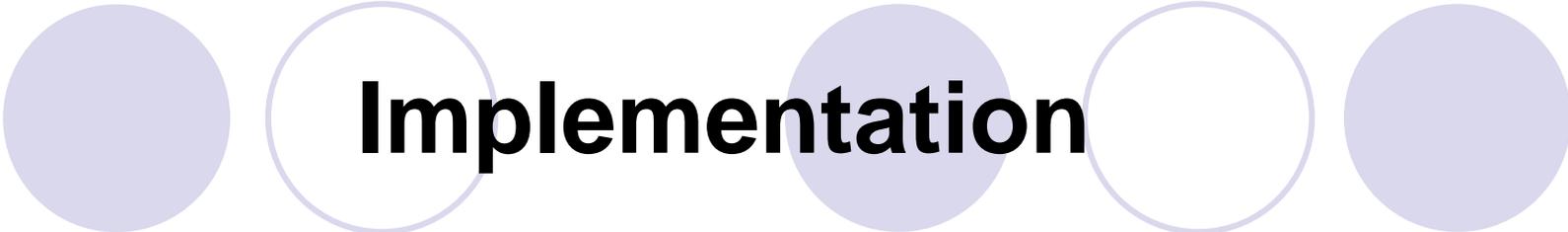
- Appointing a COOP Coordinator
- Organization of a COOP Team
- Initial Project Meeting

# Identification of Functional Requirements

- Identifying essential functions
- Identifying vital records, systems and equipment
- Naming key personnel
- Selecting an alternate facility
- Determining the existence of interoperable communications

# Design and Development

- Decide whether the plan will consist of one large plan or a series of smaller COOP plans.
- Place collected data into a COOP plan draft.

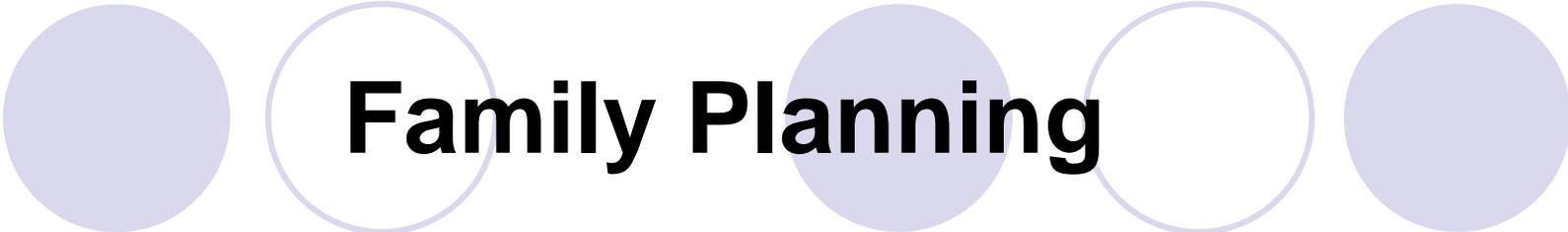


# Implementation

- COOP Plan put into practical effect.
- To ensure the support of all employees, the implementation phase of the COOP planning process needs to address the following two issues:
  - Human Capital Management
  - Family Planning

# Human Capital Management

- Places the right people in the right jobs to perform the agency's essential functions most effectively.
- Ensures that all employees have a clear understanding of what they are to do in an emergency.
- Includes specific protocols for identifying and assisting special-needs employees.

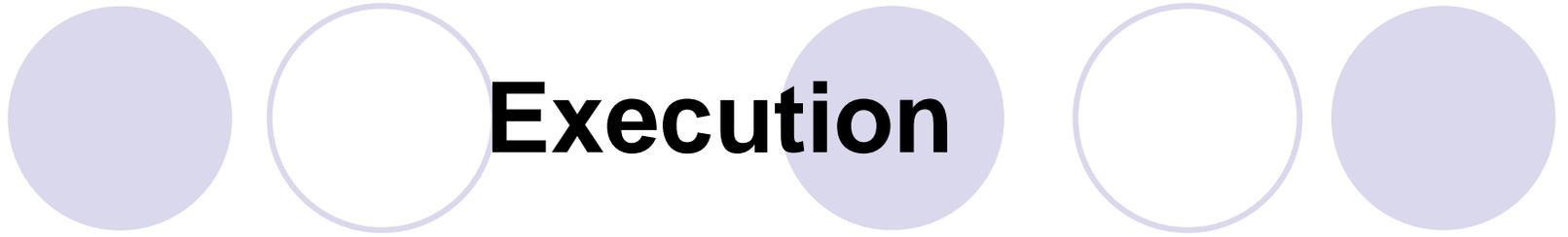


# Family Planning

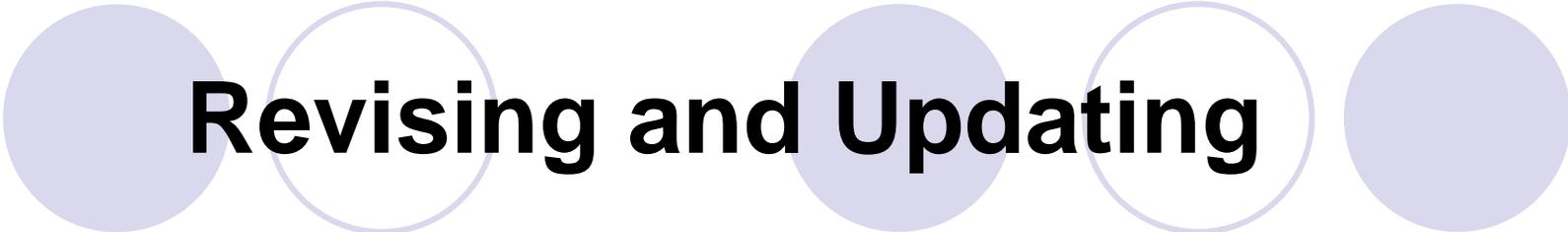
- Developing a plan
- Creating a Go-Kit

# Training, Testing and Exercises

- Assess and validate COOP plans, policies and procedures.
- Ensure that agency personnel are familiar with COOP procedures.
- Ensure that COOP personnel are sufficiently trained to carry out essential functions in a COOP situation.
- Test and validate equipment to ensure both internal and external interoperability.



- Building Evacuation Plan
- Emergency Response Team
- COOP Execution



# Revising and Updating

- Training key personnel.
- Conducting periodic COOP exercises.
- Institution of a multiyear process to ensure the plan continues to be updated as necessary.

# State COOP Planning Strategy

- COOP was integrated into the Commonwealth of Virginia Emergency Operations Plan.
- The scope of evaluation was narrowed to the 45 Virginia Emergency Response Team (VERT) agencies.
- VDEM developed a COOP Planning Manual to serve as both a standard and guidance for state agencies to use.
- Partnering with an outside consultant VDEM built a crosswalk assessment tool using National Fire Protection Association (NFPA) 1600, Emergency Management Accreditation Program (EMAP) Standards (2004), FEMA's Interim Guidance to State & Local Governments and FPC 65.
- With the crosswalk, the consultants conducted an assessment of each VERT agency's COOP plan, including a one-on-one session.



# State COOP Program

- In October 2005, EMAP Assessors reviewed the crosswalks, VERT agency plans and the VDEM COOP Planning Manual.
- On November 16, 2005, Virginia was awarded full accreditation and the VDEM COOP Planning Manual was cited as a “Best Practice.”

# State COOP Program Development

- **Authorities**

- § 44-146.18 of the Code of Virginia (2005)

- Tasks VDEM with providing guidance and assistance to state agencies and local governments in developing and maintaining COOP programs, plans and systems.

# State COOP Steering Committee

- Provides the principal inter-organizational forum for discussion of COOP matters, such as:
  - Dissemination of information
  - Managing inter-agency dependencies
  - Coordinating COOP exercises including inter-agency exercises
  - Accommodating ongoing legal and regulatory requirements
  - Facilitating the overall COOP program and project plans along to include the supporting financial/budget plan for the Commonwealth, and
  - Conducting periodic assessment of statewide COOP capabilities and reporting the results to the Governor.



# State COOP Program

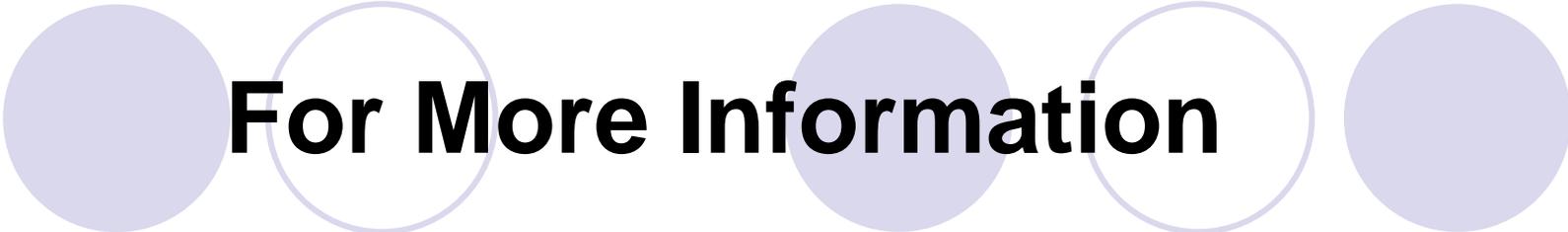
- VDEM provided training on *How to Develop a COOP Plan Using the VDEM COOP Planning Manual*
- VDEM created the COOP Toolkit, an on-line resource posted on the VDEM webpage, [www.vaemergency.com](http://www.vaemergency.com).

# Commonwealth of Virginia Guidance

## VDEM COOP Tool Kit

[www.vaemergency.com](http://www.vaemergency.com)

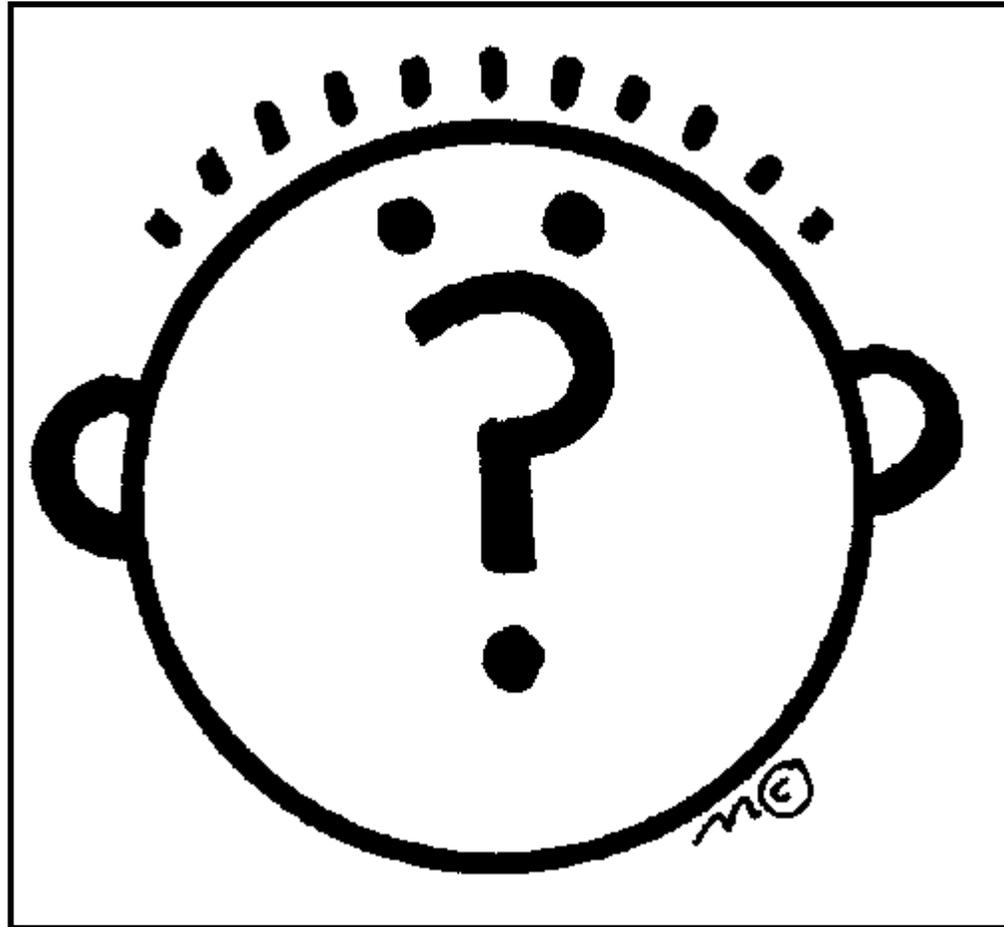
The screenshot displays a Microsoft Internet Explorer browser window with the address bar showing <http://www.vaemergency.com/library/coop/index.dfm>. The website header includes the VAEmergency.com logo and navigation links. The main content area is titled "Library" and features a "Continuity of Operations Planning Toolkit" section. This section includes links to "COOP Toolkit Home", "COOP Resources", "Lessons Learned", "COOP Steering Committee", "COOP Funding", and "COOP Contacts". Below this, there is a "COOP Toolkit" section with a description: "Continuity of Operations ensures the stability of essential functions through a wide range of emergencies and disasters. Today's changing threat environment and recent natural and man-made emergencies demonstrate the need for COOP capabilities and plans at the local, state and federal levels." Further down, it mentions Executive Order 7 (2002) and Executive Order 69 (2004). A red banner at the bottom of the page reads "Working to Protect People, Property and Our Communities". The footer contains the text "www.VAEmergency.com: Virginia's Emergency Web site", "© 2006, Virginia Department of Emergency Management", and "WAL Level A Compliant". The browser's taskbar at the bottom shows several open applications, including "Inbox - Microsoft Out...", "VEMAConferenceCE", "Presentation2", and "VAEmergency.com > ...".



# For More Information

- Federal Preparedness Circular (FPC) 65
- FEMA, Introduction to State and Local EOP Planning Guidance, August 2002
- FEMA Independent Study Program: IS-547 Introduction to Continuity of Operations (COOP)
- FEMA Independent Study Program: IS-546 Continuity of Operations (COOP) Awareness Course
- FEMA Interim State/Local COOP Planning Guidance, May 2004

# Questions?





# OFFICE OF COMMONWEALTH PREPAREDNESS

Curtis Brown

Office of Commonwealth Preparedness

[Curtis.Brown@Governor.Virginia.Gov](mailto:Curtis.Brown@Governor.Virginia.Gov)



# Office of Commonwealth Preparedness

- ◆ Codified in 2006 General Assembly

- ◆ Office's Mission:

- Provide oversight, coordination, and review of all disaster, emergency management, and terrorism management plans for the state and its agencies.*

- Coordinate working relationships between state agencies and the Governor's Cabinet.*



# Activities/Initiatives

- ◆ *2006 State Agency Preparedness Survey*
- ◆ *Preparedness as an component of each Agency's Mission*
- ◆ *Increased Focus on COOPs and Coordinating Statewide Preparedness Strategy (IT Essential)*
- ◆ *Provide a long-term roadmap for VA's preparedness through an enterprise-wide, all-hazards approach*



# Office of Commonwealth Preparedness

Patrick Henry Building  
1111 E. Broad Street, 3<sup>rd</sup> Floor  
Richmond, VA 23219  
(804) 692-2597, (804) 225-3882-fax



Virginia Information Technologies Agency

# VITA COOP PLANNING

Barbara Vaughan, VITA

---

ISOAG Meeting

Date September 20, 2006

**expect the best**



## History of Planning Efforts

- SunGard contract since 1994 for MVS mainframe & 1996 for Unisys mainframe
- Special Team did Y2K Planning & Preparations
- Current SunGard contract signed in 2000 covers both MVS & Unisys mainframes, the VITA Central network & Windows & Unix servers as required
- Emergency Response Procedures developed in late 2001 (became a part of the COOP plan)
  - Names an Emergency Management Team to act at time of disaster (Executive Team)
  - Defines Authority to implement as well as Succession of Authority
  - Documents the steps in Activating an Emergency Response



## Business Impact Analysis (BIA)

- Conducted by DIT in 2002
- Cross-functional teams
- Essential functions of DIT determined – approximately 60 business processes
  - Risk Assessment (RA) done on essential processes
- Report issued in October 2002



## COOP Efforts

- Began after completion of BIA
- Teams set up by major functions
  - Administrative
  - Data Center
  - COV Critical Services & Support of Customer Applications
  - Customer Requests & Management of Business Partner Arrangements
  - Procurement
  - Internal Hardware & Software Support
  - Network
- Team Leaders and Team Members were assigned based on functions performed not by directorate



# VITA Central Teams & Members

- Administration – Renea Dickerson, Leader  
Anne Cowles Dana Smith Paul Hoppes Alvin Seay
- Data Center – Bob Pontius, Leader  
Vickie Childress Kevin Kelley Deborah Benniefield  
Wendy Hudson Deborah Lewis Charlean Murray  
Ed Green Cindy Bryce
- COV Critical Services & Support of Customer Applications – Michael Treagy, Leader  
Pat Jeffries Barbara Garnett
- Customer Requests & Management of Business Partner Arrangements – Brenda Batkins, Leader  
Margaret Moran Vickie Rash  
Patti Barker Deborah Workman
- Procurement – Carmen Holmes, Leader  
Juliet Nisley Peter Batley
- Internal Hardware & Software Support – Mike Elliott/Jamey Stone Leader  
Bill Tyson Bob Collier Thomas Clark
- Network, John Perkins, Leader  
Tom Simpson Billie Jean Schultz  
Charlotte Tabb Al Clark



## Data Center Recovery

- VITA Infrastructure to include mainframes, network, routers, switches, etc.
- Agency-specific hardware if covered on the SunGard contract
- Operating systems recovered so that agencies can restore applications supporting essential business functions



## VITA COOP EFFORTS (continued)

- Recovery Procedures developed for all essential functions
- Procedures include hardware, software and personnel resource requirements
- Procedures are reviewed and updated quarterly
- BIA reviewed and updated annually (June)
- Desktop exercises conducted annually (last done in November 2005)
- Exercise of data center recovery conducted at SunGard annually (last done in April 2006)



# SunGard Contract Coverage

- Richmond Plaza Building Data Center
- VITA agency locations that have determined the need for SunGard backup
  - VDOT – Central Office
  - DPOR – applications at its location
  - SBE – email servers
  - DRS – one server
  - DSS – one server
- Agency-specific hardware in the RPB Data Center
  - DSS – Primepower 1500 (E10000)
  - TAX – Servers for iFile & IRMS
  - SCC - router
  - DMV - routers
  - DMAS – router
- VITA pays SunGard \$210,304 monthly of which agency-specific costs are \$51,141
- Modified quarterly if needed to assure current hardware configurations are available



# Disaster Declaration at SunGard

- Decision made collaboratively by VITA and Northrop Grumman
- Disaster Declared using SunGard established procedures by VITA designees
- Declaration Fees - \$75,000 for MVS; \$20,000 for Unisys; \$20,000 for E10000; \$2,500 for Server Group
- Daily Usage Fees – \$45,000 for MVS; \$5,000 for Unisys; \$5,000 for E10000; for Server Group – no usage fee for 1<sup>st</sup> 30 days



# Backup Generators

- Contract with Carter Machinery
  - Provides for 2 diesel generators within 6 hours of notification to be hooked at RPB
    - Provide power to run the VITA data center (raised floor only) and one HVAC and cooling tower for chilling the water required by the system
  - Provides for a supply of fuel for as long as the generators are needed by VITA
  - Monthly fee - \$9,000
  - Activation fee - \$17,679 (minimum 1 day) - \$76,890 (maximum for 5 days)



# Current COOP Planning Efforts

## Short-Term Objective

Begin to revise the VITA COOP to encompass VITA Customer locations' needs in the current environment by January, 2007

## Long-Term Objective

Begin to develop a detailed written plan to complete a VITA Enterprise COOP in accordance with existing VDEM standards. VITA COOP Team has been formed and met on September 19.



## Short-term COOP Planning Efforts

- Revised VITA COOP Plan to encompass the agency location plans into the VITA IT Recovery plan
  - Collected IT Recovery Plans from customer agencies
  - Using a regional approach with emphasis being placed on the Eastern region
    - Created a procedures/reporting document for regional staff to follow for emergency response
    - Created emergency response call trees for all regions



# Long-term COOP Planning Efforts

- COOP Planning Team has been named and met September 19.
- Project plan developed for a VITA Enterprise COOP Plan
  - Follow guidelines established by VDEM
    - Conduct a BIA to replace the one completed in 2002
      - Formation of VITA necessitates that the COOP plan include IT infrastructure support for all agencies. A gap analysis of agency-based IT recovery plans will be done using a disaster recovery template based on VDEM guidelines. The results will be used in working with agencies to develop more comprehensive recovery plans for agency-based locations.
      - New directorates at VITA
      - New functions at VITA
      - IT Partnership with Northrop Grumman (NG)
- NG's Evaluation of VITA's recovery plans, SCD+90
- Office of Commonwealth Preparedness & VDEM advocate planning efforts be by the 7 Virginia State Police Regions
- New Executive Order expected



# QUESTIONS

????



# New Facilities & Disaster Recovery Solutions

Peggy Ward, VITA Chief Information Security and Internal Audit Officer

September 20, 2006



***NORTHROP GRUMMAN***

## Commonwealth Enterprise Solutions Center

Meadowville Technology Park  
Chesterfield County, Virginia



# New Facilities / Data Centers & Disaster Recovery Solutions

- Commonwealth Enterprise Solutions Center (CESC)
  - Meadowville Technology Park, Chesterfield County, Va.
- Southwest Enterprise Solutions Center (SWESC)
  - Russell Regional Business/Technology Park, Russell County, Va.
  - Future Disaster Recovery Solutions for the Commonwealth

## CESC Facility – available June 2007

- Target size of facility 192,000 S.F.
- Data center (TIER III) 50,000 S.F.
- CMOC, NOC, SOC, Technology Lab 7,000 S.F.
- Office Area 80,000 S.F.
- Common Areas 30,000 S.F.
  - Multi-purpose room (three partitioned areas / seats 260)
  - Training room (two partitioned areas / seats 40)
  - Video Teleconference / TV Production room / seats 24

# CESC Benefits to Commonwealth of Virginia, Customer Agencies and VITA

- High availability via construction of Tier III Data Center; N+1 infrastructure
- High critical systems availability / visibility from new centralized management tools
  - Customer dashboard
  - Perigrine problem management
  - HP Openview workload monitoring and management
- Lower costs / high efficiencies through consolidation
- Centralized Management Operations Center
  - Consolidated operations
  - Network monitoring and management (NOC)
  - Security Management and Monitoring (SOC)

## CESC Benefits cont.

- Home for new Commonwealth wide solutions
  - Consolidated state wide network
  - Consolidated messaging
  - Consolidated security system
- Home for agency critical systems
  - High availability / lower risk
  - Cost efficient Management
  - Customer visibility of workload
- More cost effective for disaster recovery
  - Planning and testing

## Southwest Enterprise Solutions Center

Russell Regional Business Technology Park  
Russell County, Virginia



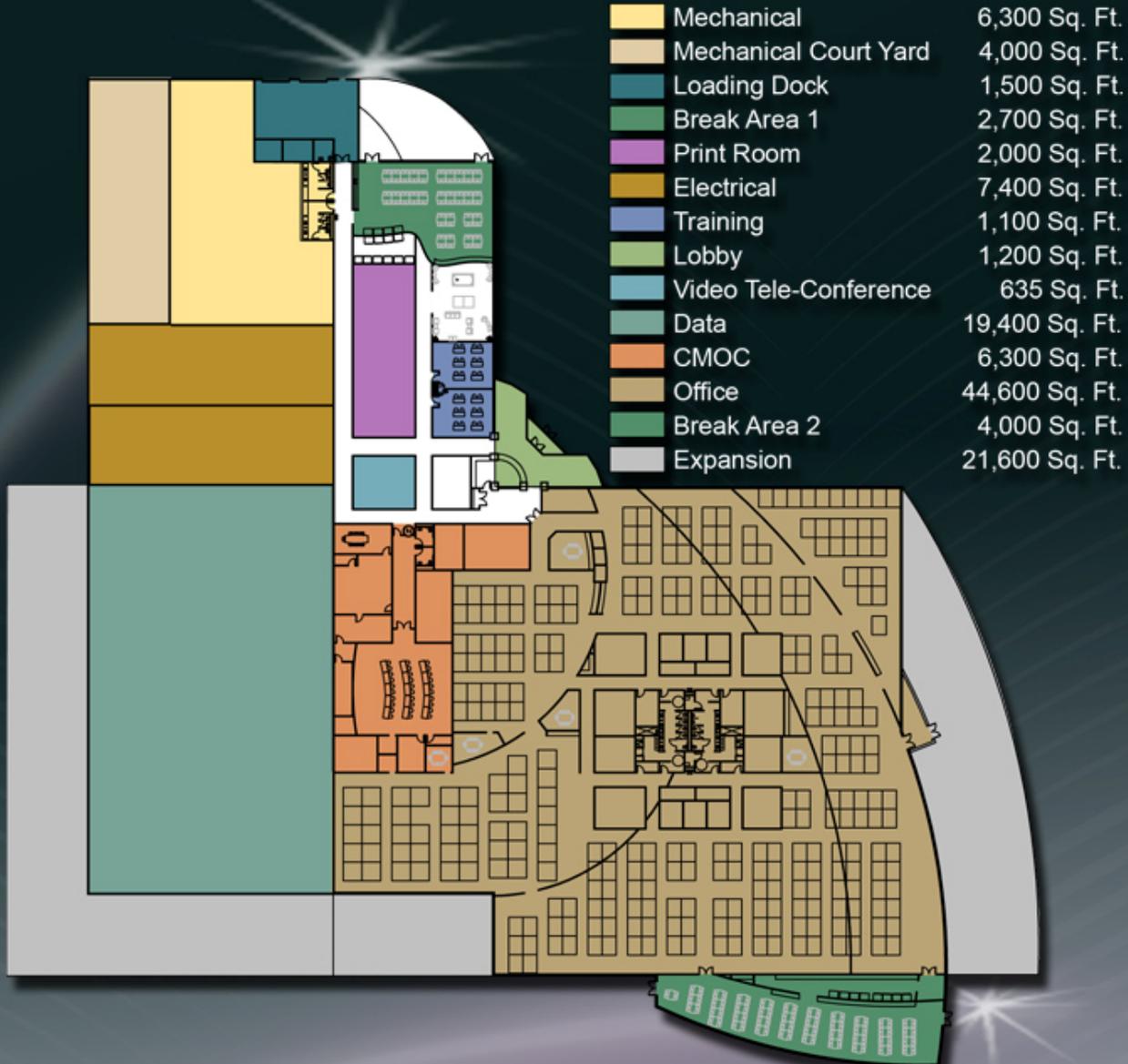




● TRI - CITES TN AIRPORT

## SWESC Facility

- Supports Economic Development of Southwest Region
  - New Facility
  - 300 + New Technology Jobs
  - Cornerstone for Technology Growth in Southwest Region



## SWESC Facility – available Oct. 2007

- **Size of facility** **101,000 S.F.**
- **Data center (TIER II+)** **20,000 S.F.**
  - Disaster Recovery Center for Commonwealth
  - Failover Messaging System
- **Office area** **48,000 S.F.**
  - Primary Help Desk / Call Center
  - Backup Consolidated Management Operations Center
- **Common Areas** **10,000 S.F.**
  - VTC
  - Training Room (seats 24)
  - Executive Conference Room



# Future Disaster Recovery Solutions for Customers

- **For all customers currently processing at RPB & on SunGard Contract:**
  - Disaster Recovery at SWESC
  - Hardware / Software / Network in place at SWESC for fast recovery
  - Data Replication and recovery within 24 hours (vs current 72 hrs)
  - Messaging failover at SWESC for continued service
  - Back-up CMOC / NOC / SOC in place for continued operations
  - Primary help desk at SWESC for continued service
  - Test at customer convenience (not locked into SunGard)
- **Environment in place for new customers (not on SunGard Contract) — Requires Funding:**
  - Business Impact Analysis (BIA)
  - Disaster Recovery Test Plan
  - Performance of periodic test



# Commonwealth Information Security Officers Meeting

**Fred Duball**  
September 20, 2006



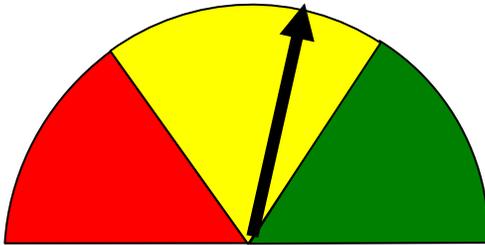
# 90 Day Outlook – Transformation Milestones

Ref. # (Schedule 10.1.2)tem	Description	Due Date	Status
59	Incident management system web accessible	8/1/06	Implementation Plan Delivered 8/1 <a href="#">Implementation in-process</a>
4	Procedure Manual Plan	8/1/06	Implementation Plan Delivered 8/1 <a href="#">Implementation in-process</a>
5	Procedure Manual (Critical)	10/01/06	On schedule Acceptance criteria in review.
3	Knowledge Management System Operational	10/01/06	On schedule. Acceptance criteria feedback received from VITA.
53	Interim Security Incident Tracking and Management System	10/01/06	On schedule Acceptance criteria in review.
9	Infrastructure Operation Center (interim) (Operational Implement HPOV)	11/01/06	On schedule Acceptance criteria in review.
34	Temporary NOC	11/01/06	On schedule Acceptance criteria in review.



NORTHROP GRUMMAN

# Transformation Dashboard



**Explanation:** Data collection process being assessed for the best method to result in validated and quantified data. RFP for hardware, services and Enterprise License Agreement strategy in process. Accelerated Altiris Backend Infrastructure schedule.

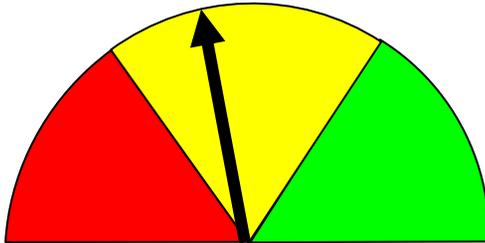
**Recovery Date Y-->G: Week of 9/28**

**Recovery Plan and Dependencies:**

- Finalize RFP for hardware and EA strategy
- Altiris backend installed early September

EUS	Desktop	Data collection process being reviewed. Enterprise License Agreement and Hardware RFP being developed for distribution. Altiris Backend Infrastructure install accelerated to complete in early September.
	Helpdesk	NG response to VITA acceptance rejection was rejected. Meeting with NG/VITA last week, awaiting VITA response. Milestone was for development system – production system being accelerated for project needs.
	Messaging	Messaging Lab hardware installed, in process of being configured.
DCS	Server	Server hardware orders in process. Storage hardware received 9/06. ITC hardware (received one rack). Servers, lab switch and remaining rack expected delivery the week of 9/11.
	Mainframe	Inventoring existing RPB hardware and software mainframe processing components. IP addressing focus team and NG Enterprise Architecture team reviewing Commonwealth's hard coded IP addressing.
	Facilities	Chesterfield County transferred the CESC land to COPT on 9/7. SWESC groundbreaking scheduled for Friday 10/27.
Network and Security Services	Data Network	Continuing to analyze VITA Agency network requirements. Awaiting confirmation that 100% of the requirements from VITA have been received.
	Voice Network	Planning being finalized.
	Security	On schedule for 10/1/06 deliverable of Interim SITMS. VAR review process in progress.
General	Cross-Functional	The 8/01 Procedures Manual Plan deliverable rejected by VITA, NG assessment underway. On track for the Procedures Manual deliverable on 10/01.
	Internal Apps	Working with Current Ops to establish clear definition for capturing SLA's for Internal Apps transformation projects (Application level SLA's). Determining Clearcase documentation reqmt's.

# Current Operations Dashboard



Explanation: ?

Recovery Date Y-->G: ~Oct 2006

**Recovery Plan and Dependencies:**

- Evaluate collection of agency facing metrics by mid Oct 06
- Evaluate agency satisfaction – Jan 07

## QoS Report (July?)

EUS	13% Desktop
	18% Messaging
	36% Help Desk
DCS	Mainframe 100%
	6% Servers
NWS	Communication – Data 90%
	0% Communication - Voice
Security	Security

Risk/Issue/ Incident	Impact	Resolution Activities
Issue: Unable to measure enterprise service levels against MOUs	Measure and monitor service delivery	Evaluate reasonable means to measure (Closure: Mid Oct)
Issue: Unable to measure agency satisfaction	Only point estimates are available to measure satisfaction levels.	Evaluation by CAMs. Inclusion of factors in yearly survey (Closure: Jan 07)
Issue: Need evaluate impact of Software AG limitations	Deployed to DOA, DMV, DIT	Evaluating impact.



# Comprehensive Infrastructure Agreement

Peggy Ward

## Partnership Audit Clauses

Virginia Information Technologies Agency



***NORTHROP GRUMMAN***

# Five Types of Assurance Services

1. **SAS 70 Type II Audit**
2. **Security Audits**
3. **Financial Audit**
4. **Operating Audit**
5. **Right to Audit**

## **SAS 70 Type II Audit (Service Provider)**

- **Scope:** Testing of controls of service delivery that may be relevant to a COV's internal control structure as it relates to an audit of financial statements.
- **Frequency:** Annual
- **Timing:** July – June (COV FY) – Report due two months after audit but not later than by Nov 1.
- **Performed by :** Third Party – Deloitte & Touche
- **Description:** Known as “Service Provider Audit”  
AICPA Statement on Audit Standards No. 70

## **SAS 70 Type II Scoping Approach – Deloitte & Touche**

**A key objective of the planning process is to evaluate the control environment**

**in a manner such that unusual or unexpected risks of potential material misstatements would be identified during the SAS70 examination. To this end, the scoping process will consider the following:**

- Financial materiality**
- Areas of financial risk (including non-material systems)**
- Interconnections between material and non-material systems**
- Risk factors repeated over time (minor risks not addressed year to year may indicate a higher level of risk)**
- Risk factors communicated by VITA or APA (user groups),**
- Other Risk Factors such as:**
  - Regulatory requirements**
  - Potential sources of negative publicity**
- Randomness (some non-material systems may be selected at random)**
- Contractual requirements**

## **SAS 70 Type II Scoping Approach – Deloitte & Touche**

**The planning process will utilize several inputs in order to make determinations regarding the scope of processes and controls to**

**be considered. The following list reflects several of the inputs that Deloitte & Touche expects to include:**

- Interviews with VITA/NGIT personnel**
- Analysis of Security Survey Completed by VITA**
- Interviews of key Agency personnel (AITR, ISO and Internal Audit) coordinated through VITA Customer Relationship Management (CRM)**
- Examination of VITA and Agency documentation**
- Feedback from the APA concerning applicability to financial audits**

# Security Audits

- **Scope: Every infrastructure location**
- **Frequency: Relative to Risk, Annual Plan – report within two weeks of review.**
- **Timing: Annual plan – multiple reviews**
- **Performed by : Third Party – Deloitte & Touche**

# Financial Audit

- **Scope: Payment and Invoicing**
- **Frequency: Annual**
- **Timing: July – June (COV FY) – Report due two months after audit but not later than by Nov 1.**
- **Performed by : Third Party – Deloitte & Touche**

# Operational Audit

- **Scope: Determined Annually**
- **Frequency: Annual**
- **Timing: July – June (COV FY) – Report due two months after audit but not later than by Nov 1.**
- **Performed by : Third Party – Deloitte & Touche**

## Right to Audit

- **Scope: As needed**
- **Frequency: As needed**
- **Timing: As needed**
- **Performed by : APA, JLARC, DOA or VITA Internal Audit**

?

# QUESTIONS

?



Virginia Information Technologies Agency

# Protecting Sensitive Data

Cathie Brown, VITA

---

ISOAG Meeting

Date September 20, 2006

**expect the best**



## Sensitive Data

Recent Breaches = ++ CONCERN ++

- COV ITRM Security Std SEC501-01: DO NOT store sensitive data on mobile devices, including laptops!! IF YOU MUST, there must be a documented business necessity in writing approved by the Agency Head including mitigating controls in place (such as authentication & encryption). Compliance date = July '07; however, earlier compliance with this section is strongly encouraged!
- Sensitive Data = “any data of which the compromise with respect to confidentiality, integrity, and/or availability could adversely affect COV interests, the conduct of Agency programs, or the privacy to which individuals are entitled.”



# Types of Sensitive Data

Examples of types of sensitive data include:

- Personally Identifiable Information including information that describes, locates or indexes anything about an individual including financial transactions, social security numbers, medical history, ancestry, religion, political ideology, criminal or employment record & photographs,
- Proprietary research data,
- Certain confidential proprietary data,
- Network diagrams & IP addresses,
- Server names and configurations, &
- Contract cost estimates.



## Limit Collection

- Best Defense = DO NOT collect sensitive data unless an absolute business necessity.
- If it must be collected, see if collecting only a portion is a viable option such as the last 4 digits of a credit card # or SSN.



## SAFEGUARD Sensitive Data

- If sensitive data must be collected & stored, implement appropriate safeguards commensurate with the level of sensitivity and risk.
- Consider the controls over sensitive data in motion (being transmitted) and sensitive data at rest (stored).



## Sensitive Data in Motion

- DO NOT transmit via email which is not secure unless encrypted.
- DO NOT transmit electronically unless encryption is used!
- For web entry always look for the yellow lock at the bottom right as well as the Https in the address indicating Secure Sockets Layer.



## Sensitive Data at Rest

Storage of sensitive data should be in the least mobile location as possible & adequate technical controls should be deployed. Some available controls:

- 2-factor authentication via software or hardware token such as a Kfob,
- Complex passwords that require a combination of upper case, lower case letters, numbers, and/or special characters,
- Mandatory screen saver passwords,
- Encryption, &
- Physical protection of mobile devices that can be easily moved such as a PDA, blackberry or laptop.



# Your Sensitive Data

Finally, for your own protection:

- Do not provide your personal data electronically including via the web or email unless you are absolutely positive it is encrypted and the recipient is valid.
- Do not respond to unusual emails or click on unrecognized URL's.
- Keep your personal computer updated for the latest patches and anti-virus definitions.

**!Trust but verify!**



## Additional Information

For additional information

- VITA Security

<http://www.vita.virginia.gov/security/security.cfm>

- MS-ISAC: <http://www.msisac.org>

- U.S. Department of Homeland Security's  
US-CERT: <http://www.uscert.gov>

- NCSA: [www.staysafeonline.info/](http://www.staysafeonline.info/)



# QUESTIONS

????



## OTHER BUSINESS

Any Items for  
Discussion??



**ADJOURN**

**THANK YOU FOR  
YOUR TIME AND  
THOUGHTS**

**!!!**