



Department of Veterans Affairs
Office of the Assistant Secretary for Information and Technology
Office of Cyber Security



Cyber Security Requirements

(Securing the VA Enterprise)

A Presentation to the National CIO Conference

October 29, 2001



Bruce A. Brody, CISSP
Associate Deputy Assistant Secretary
for Cyber Security
202-273-8007
Bruce.Brody@mail.va.gov



Mission

- ? **Provide cyber security services to veterans and their dependents that protect the confidentiality, integrity and availability of their private information and enable the timely, uninterrupted and trusted nature of those services.**
- ? **Provide assurances that cost-effective cyber security controls are in place to protect automated information systems from financial fraud, waste and abuse.**



As the Associate Deputy Assistant Secretary for Cyber Security, I am accountable for the Department's accomplishment of this mission.



Historical Perspective

VA's history of cyber security challenges have contributed to significant pressure to make fundamental changes in managing our information systems.

There appear to be four basic causes of our historical cyber security problems:

- Decentralization inconsistencies,
- Lack of previous management support,
- Inadequate or splintered funding, and
- Inattention to responsibilities.





Fundamental Information Security Weakness

The *oversight community* considers information security in the VA to be a “material weakness” –

*The lack of adequate controls over VA Automated Information Systems (AIS) place critical VA operations at risk of **inadvertent or deliberate misuse, fraudulent use, improper disclosure or destruction, possibly occurring without any detection** in areas such as:*

- *financial management and transaction data,*
- *health care delivery and medical records,*
- *personal information and benefits, and*
- *life insurance services.*

Report of Audit of the Department of Veterans Affairs Consolidated Financial Statements for Fiscal Years 2000 and 2001





What GAO and the OIG Are Telling Us



The “material weakness” derives primarily from the failure to properly engineer and implement information security in our enterprise.

- Failure to provide adequate entity-wide security controls,
- Inadequate access controls,
- Inadequate controls over software applications,
- Inadequate controls over segregation of duties,
- Inadequate controls over system software, and
- Inadequate attention to continuity of operations planning and preparation.



Federal Information Systems Control Audit Manual (FISCAM)



The Complexity of the Challenge

In addition to FISCAM, a growing body of laws and requirements are being imposed on a VA cyber security structure that cannot absorb them....

-  **FISCAM**
-  **FMFIA**
-  **FITSAF**
- GISRA/OMB A-130**
-  **Zachman Architecture Framework**
-  **NIST/NIAP/NSA Standards and Guidelines**
- Policies**
- Best Practices**



- Who is accountable?
- Are we GISRA compliant?
- What is our FITSAF level?
- Who accepts the risk?
- Which system or facility should be protected first?
- Which systems contribute to the material weakness?
- How do we get a system certified and accredited?
- Where do we turn for guidance?
- Who's in charge?



Beginning to Solve the Problem



The Secretary has made it clear that he expects these problems to be fixed and is providing leadership and commitment in multiple initiatives.



- The CIO and Deputy CIO are providing direct management support;
- Funding for initiatives that cross Administrations must be adequate and centrally managed;
- Individual and collective cyber security responsibilities and accountability must be resolved; and
- VA's Enterprise Architecture, the IT Security Capital Plan and the outputs from the GISRA reviews will provide the pathway for correcting the cyber security "material weakness."



Assigning Accountability and Responsibility

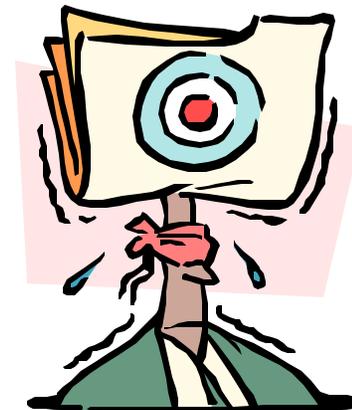


- **Secretary's April 9, 2001 memorandum on SES performance plans assigns senior-level accountability:**

Program managers must exercise due diligence or care in their efforts to plan, develop, coordinate, and implement an effective information security program.

- **Secretary's July 25, 2001 memorandum on IT Governance defines the authority of the Department CIO vis-a-vis Administration CIOs**

- Technology direction and guidance
- Funding approval
- Input to performance evaluations





The Department's Cyber Security Priorities



- **Remove the “material weakness” within 2 years**
- **Comply with all GISRA (and OMB A-130) requirements**
- **Lay the security groundwork (including Defense-in-Depth) for implementing the VA Enterprise Architecture**
- **Achieve Federal CIO Council and NIST FITSAF Level 4 and get on a trajectory to Level 5**
- **Become a model cyber security program in the Federal Government**

All of which ensures the confidentiality, integrity and availability of veterans' private information, and assures that our systems are free from financial fraud, waste and abuse.



A Few Key Office of Cyber Security Programs

- **Security for the Enterprise Architecture**
 - Security meta-framework of the Zachman Framework
 - Defense-in-Depth
- **VA Central Incident Response Capability (VA-CIRC)**
- **Certification and Accreditation**
- **Public Key Infrastructure (PKI)**
- **IT Security Capital Plan**
- **GISRA**
- **Office of Cyber Security Reorganization**



Your Participation and Cooperation are Required.

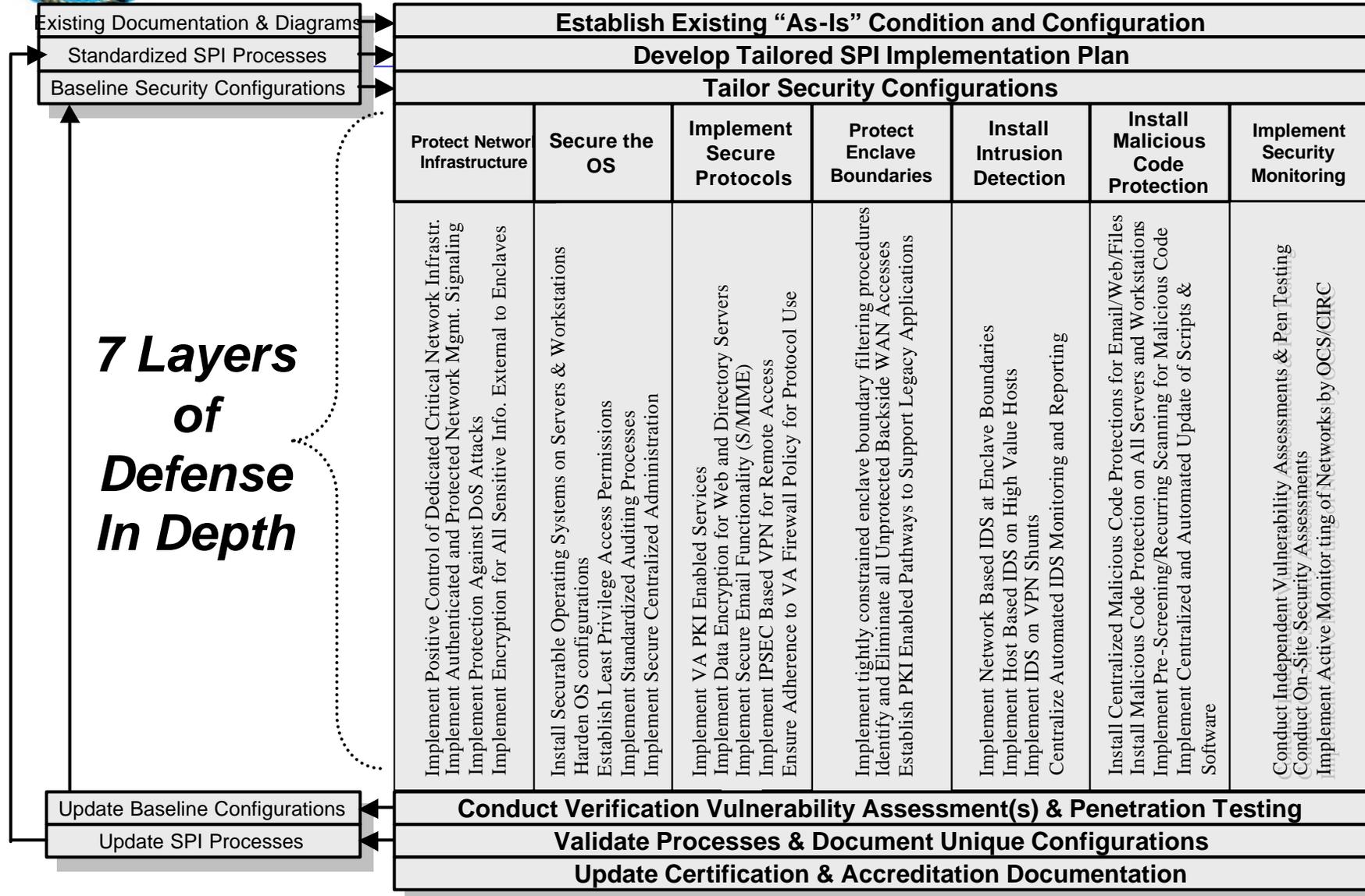


Enterprise Architecture

Perspective/Model	Data	Function	Network	People	Time	Motivation
Planner/Scope	<ul style="list-style-type: none"> ?? Veterans ?? Information Exchange ?? Care Givers ?? Insurers/Claims ?? Lenders ?? Employees ?? Laws/Executive Orders 	<ul style="list-style-type: none"> ?? Access Controls ?? Application and System Software Controls ?? Entity-wide Security Controls ?? Continuity of Business Operations ?? System Security Certification & Accreditation ?? Risk Abatement 	<ul style="list-style-type: none"> ?? VA IT/Data Centers ?? VA Central Offices ?? VHA Patient Care Centers ?? VBA Regional Offices ?? NCA Cemeteries 	<ul style="list-style-type: none"> ?? Office of the CIO ?? Office of Cyber Security Organization ?? VA CIRC ?? FBI CERT ?? Other External Security Organizations ?? Other Internal Security Organizations ?? Segregation of Duties 	<ul style="list-style-type: none"> ?? Response to New Security Law, Regulation, or Executive Order ?? Identification of new: <ul style="list-style-type: none"> ?? Insurer ?? Care Giver ?? Lender 	<ul style="list-style-type: none"> ?? Achieve & Preserve Information Security ?? Satisfy Existing Laws and Executive Orders Relating to Information Assurance (E) ?? Cyber Security Capital Planning (M)
Owner/Business Model	<ul style="list-style-type: none"> ?? VA Enterprise ?? Networks ?? Applications ?? Hosts ?? Business Entities & Relationships ?? ITSS ?? VHA/VBA/VCA ?? Information Classification 	<ul style="list-style-type: none"> ?? Process Flow diagrams for the above ?? Secure and Reliable Information Exchange ?? Process Classification ?? GISRA Audits ?? Security Training ?? Security Monitoring 	<ul style="list-style-type: none"> ?? VA Data Networks Mapping ?? Data Link ?? Network ?? VA Distributed Application Architecture ?? System Classification 	<ul style="list-style-type: none"> ?? Security Management Framework ?? Organization Structure, CONOPS, and Work Products of Cyber Security Organization ?? Organization Structure, CONOPS, and Work Products of CIRC Organization ?? VA Enterprise Cyber Security Governance ?? ISO Process and Procedures ?? Trust Model/Relationships 	<ul style="list-style-type: none"> ?? ITSCAP Cycle ?? Security Definition ?? Verification ?? Validation ?? Post Accreditation 	<ul style="list-style-type: none"> ?? Cyber Security Organization Business Plan ?? Core Security Principles (E) ?? Cyber Security Goals and Objectives (E) ?? VA Security Directives (M) ?? PKI Strategy (M) ?? Threat Assessment (M)
Designer/System Model	<ul style="list-style-type: none"> ?? Cyber Security Technical Architecture Handbook ?? Security Standards Profile ?? Open System Security Standards ?? Health Care Industry Security Standards 		<ul style="list-style-type: none"> ?? Defense-in-Depth Layers ?? Design documents for <ul style="list-style-type: none"> ?? Network View ?? Host View ?? Application View 	<ul style="list-style-type: none"> ?? Cyber Security Operations Guide ?? Permissions Model for System/Information Read/Write/Create/Delete ?? Security Monitoring <ul style="list-style-type: none"> ?? Network ?? Host ?? Applications 	<ul style="list-style-type: none"> ?? Security Processes & Plans, e.g. <ul style="list-style-type: none"> ?? Security Incident Response Process ?? Technology Refresh Process ?? Business Continuity Plan ?? Disaster Recovery Plan 	<ul style="list-style-type: none"> ?? VA Security Handbooks (E) ?? System Security Plan (M) ?? Risk Assessment (M)
	<ul style="list-style-type: none"> ?? VA Security Methods ?? Confidentiality ?? Integrity ?? Availability 	<ul style="list-style-type: none"> ?? System Diagrams for all of the above ?? Functional Specifications for all of the above ?? Security Controls Specifications 				
Builder/Technology Model	<ul style="list-style-type: none"> ?? Data storage, interchange, & reporting standards for security incidents and intrusion detection 	<ul style="list-style-type: none"> ?? PKI ?? Identification & Authentication Process ?? Access Control Process ?? Non-repudiation Process ?? Malicious Code Detection & Containment ?? Alerting ?? Audit Log Processing ?? Backup Processing 	<ul style="list-style-type: none"> ?? Selected technologies for <ul style="list-style-type: none"> ?? Encryption/VPN ?? Firewalls ?? Access ?? App. Security 	<ul style="list-style-type: none"> ?? Procedures Manuals ?? Firewall Reconfiguration ?? System Security Audits ?? Forensic Analysis ?? Crew Position Training, Certification, and Operators Manuals 	<ul style="list-style-type: none"> ?? Subprocesses for the above, e.g. <ul style="list-style-type: none"> ?? Event Response Procedures ?? PKI RA Processes & Procedures 	<ul style="list-style-type: none"> ?? Availability & Performance Objectives (E) ?? Best Security Practices (M), e.g. <ul style="list-style-type: none"> ?? PKI Certificate Policy ?? PKI Certificate Practices Statement
Subcontractor/Components	<ul style="list-style-type: none"> ?? System Component Security Databases 	<ul style="list-style-type: none"> ?? Detailed Inventory of Security HW/SW Components, Configurations, Versions 	<ul style="list-style-type: none"> ?? Detailed Location and Connectivity of HW/SW Inventory 	<ul style="list-style-type: none"> ?? Positive Identification/ Authentication of Individuals and their role 	<ul style="list-style-type: none"> ?? Steps for the above, e.g. <ul style="list-style-type: none"> ?? Crew Position Activity Checklists 	<ul style="list-style-type: none"> ?? System Certification and Accreditation (E) ?? Crew Position Certification Requirements (M)



Defense-in-Depth





VA Central Incident Response Capability (VA-CIRC)



- **OMB Circular A-130, Appendix III, requires that all Federal agencies establish a CIRC that interfaces with the FedCIRC**
- **There is one CIRC in the VA – no intermediaries or filtering stops**
- **Secretary’s memo of June 18, 2001, requires reporting to the VA-CIRC by all VA facilities weekly, including negative reports**
- **CIO’s memo of August 29, 2001, states that VA-CIRC is the central location for tracking and remediating security incidents across the VA enterprise**
- **CIO’s memo of October 11, 2001, clarifies reporting requirement to VA-CIRC – ISOs report directly to VA-CIRC**
- **Failure to report to the VA-CIRC is a deficiency that contributes to the “material weakness”**
- **A new and improved “CIRC on Steroids” RFP has been prepared and will soon be released**



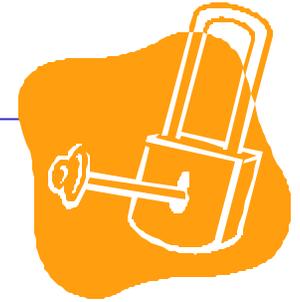
Certification and Accreditation

- **OMB A-130** requires that all Federal “SBU” systems be certified and accredited before operation
- **VA Directive 6214** has cleared coordination
 - CIO is Designated Approving Authority
 - ADAS for Cyber Security is the Certification Authority
- **Program Manager** establishes independent certification teams
- **OCS** making configuration guides, databases and other tools available for the field
- **The MITRE Corporation** has been hired to assist
- **\$290 million** requested in IT Security Capital Plan for C&A





Public Key Infrastructure (PKI)



- **VAPKI Pilot**
 - Verisign certificates
- **Office of Cyber Security currently working on a VA-wide PKI strategy**
 - Public vs. private CA, onsite vs. offsite CA hosting
 - Developing VA requirements
- **PKI technology and other access control technologies**
 - Single sign-on, smart cards, biometrics ...
- **Current phased approach**
 - Phase 1 (working groups, update policies, identify requirements)
 - Phase 2 (initial rollout, develop CONOPS, PKI integration, testing)
 - Phase 3 (training, maintenance plans, implement final PKI deployment)



IT Security Capital Plan

- **First-ever attempt to address security across all Administrations**
- **First-ever attempt to quantify the requirements of information security as a first step to resolve the “material weakness”**
- **Only the first step – another Capital Plan will be developed to account for GISRA remediation and Enterprise Architecture security requirements**
- **Biggest expenditures**
 - \$290 million for C&A
 - \$222 million for ISO salaries

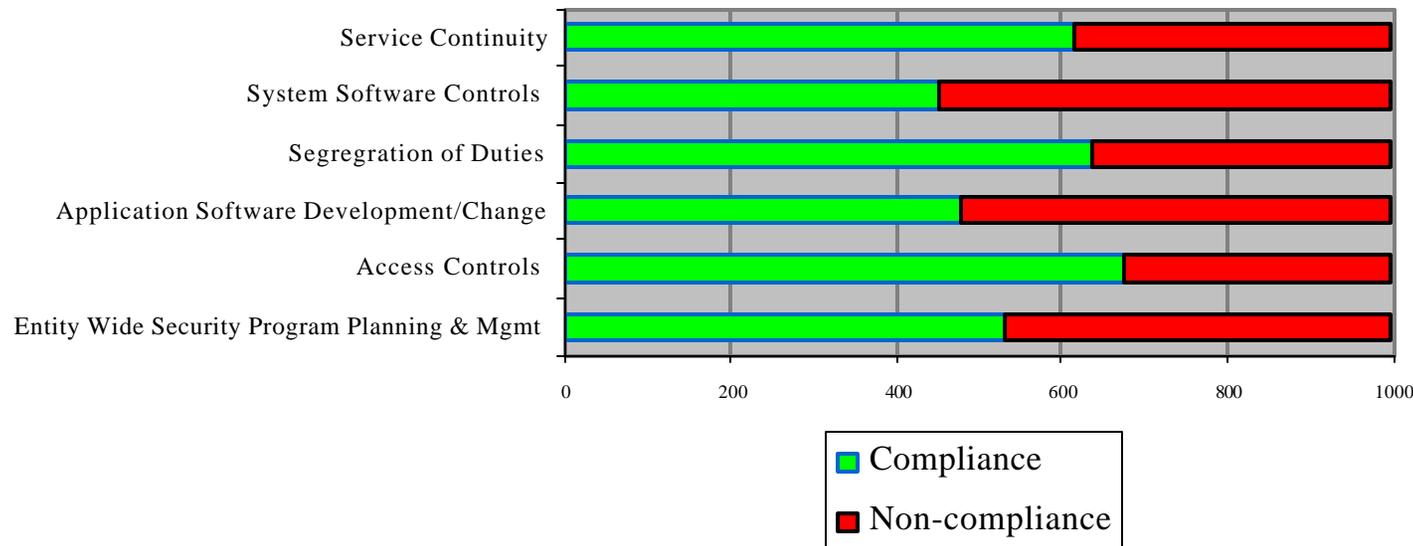




VA's GISRA Results



GISRA Results Regarding VA's Compliance with FISCAM-Mandated Controls



Using VA's unique methodology, it is possible to track single system or VA-wide compliance with the six broad FISCAM categories, but use the detailed GISRA assessment criteria.



Is Centralized Operational Control Part of the Solution?

- **The GAO thinks so**
 - Authority and responsibility commensurate with accountability
- **The Gartner Group thinks so**
 - Gartner estimates that organizations that have a variety of groups that monitor and manage security will suffer 50% more attacks than those where security management is consolidated.
 - “A fractured approach to security monitoring and management leads to security fractures.” [John Pescatore]
- **Government agencies think so**
 - Those **criticized** by Congress and GAO are decentralized
 - Defense, Commerce, Energy, Interior ...
 - Those **applauded** by Congress and GAO are centralized
 - NSA, Federal Reserve, USAID ...



Operational control to the field must be clear, unambiguous and responsive!



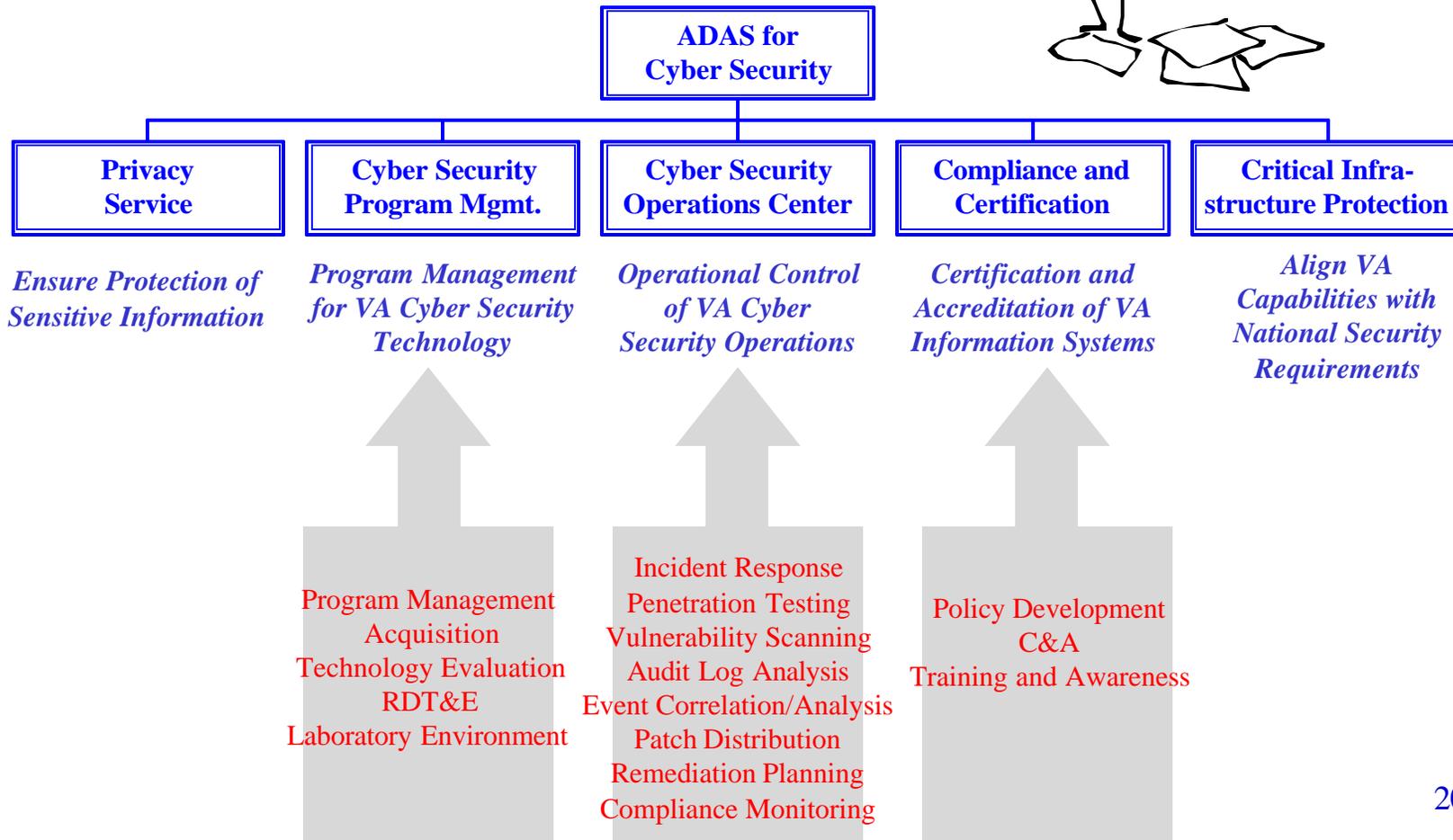
Advantages of Centralized Operational Control

- **Common set of priorities**
 - Beginning with the removal of the “material weakness”
- **Economies of scale, elimination of redundancies**
 - E.g., one database of deficiencies, not many
- **Professionalization of cyber security staff**
 - Career path, upward mobility
- **Effectiveness and coherence**
 - More likely to have a consistent and coordinated approach
- **Remote management by core team of experts**
 - Centralized controls of firewalls, IDS, patches, logs ...
- **Builds morale of technical staff**
 - Makes it easier to work in harmony
- **Helps ensure technical planning and integration needed to respond to cyber events in cyber time**
 - Seconds and minutes, not hours and days





Office of Cyber Security (To Be)





What Should You Be Doing?

- Centralized operational control of cyber security is unavoidable, so let's figure out how best to implement it
- Be responsive to one incident reporting system, one deficiency tracking system, one set of priorities and polices, and one accountable office
- Seek technical guidance and direction, and seek approval for all programs and budget expenditures, from the Office of Cyber Security – no exceptions!
- Actively report incidents (or provide weekly negative reports) to the VA-CIRC
- Seek coordination and harmony with the Office of Cyber Security on all issues – your efforts will be rewarded

I am accountable to the Department and for the Department, and I need your help.