



Virginia Information Technologies Agency



# Commonwealth Information Security Standard Update

**Michael Watson**

Chief Information Security Officer

---

Information Technology Advisory Council

Nov. 5, 2012



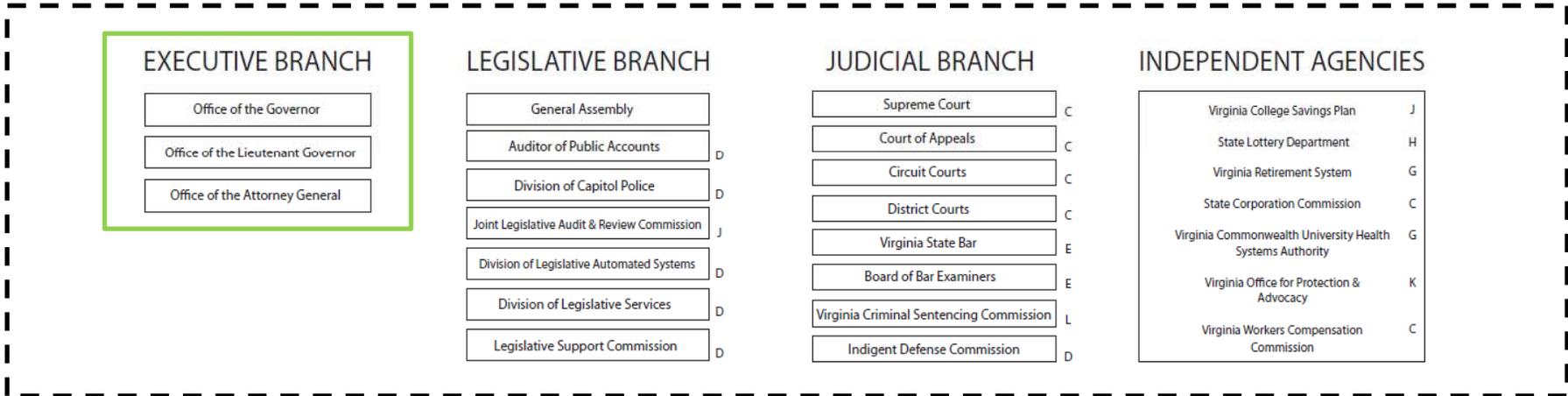


## Agenda

- Overview of the information security framework
- Discuss the major changes to the security standard
- Benefits of the changes
- Impact to the agencies



# Information Security in the Commonwealth



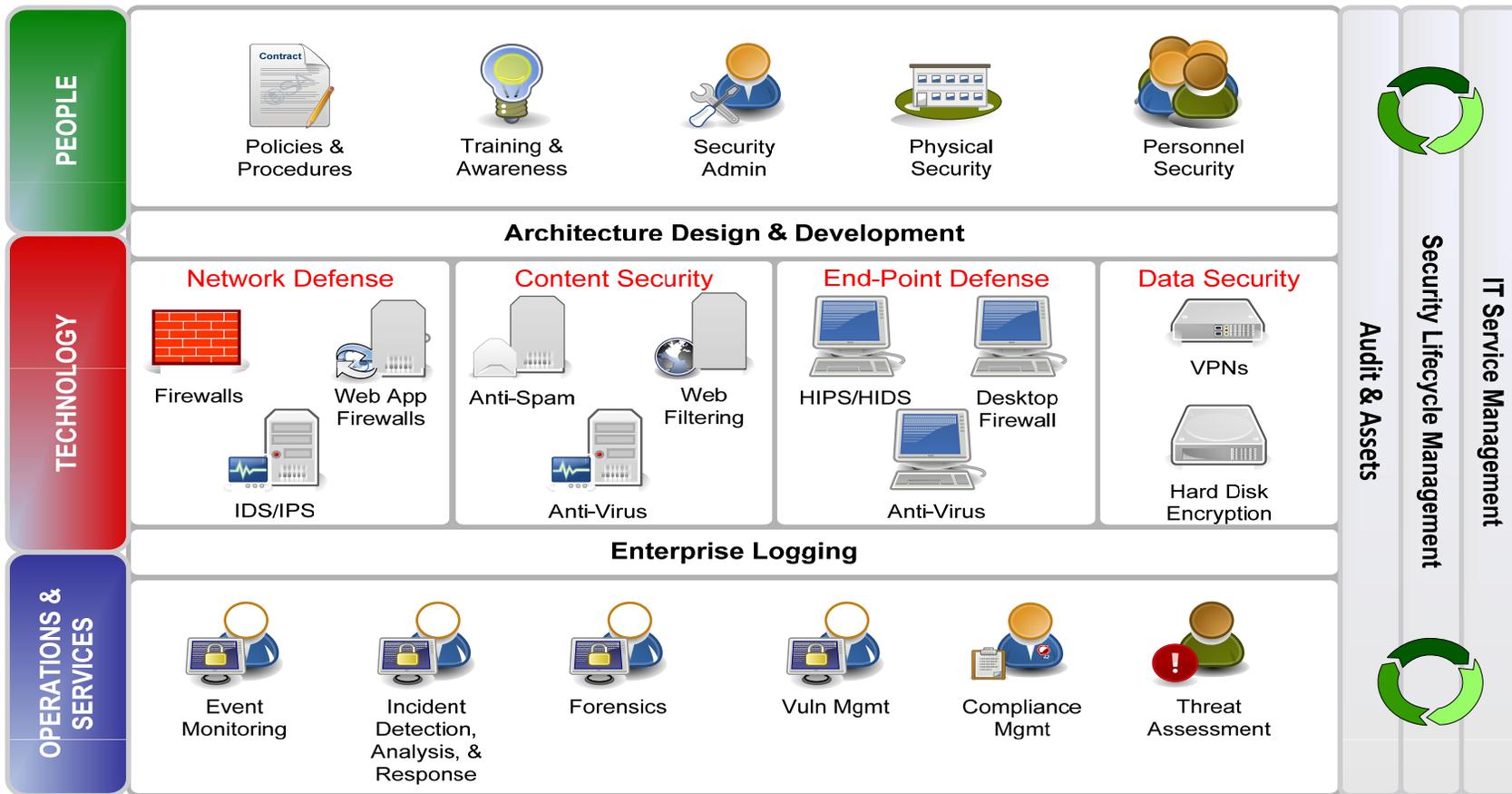
VITA is tasked with security governance over all three branches of state government



VITA manages operational security for executive branch agencies



# Security Strategy





## The Information Security Program

- Two primary documents
  - Information Security Policy (SEC500)
  - Information Security Standard (SEC501)
- Policy directives
  - Must comply with security baseline in SEC501
  - Agency head responsible for maintaining security
- Standard requirements
  - Includes required security controls to protect commonwealth data



## Updates to Security Standard (SEC501)

- Substantial restructuring of the Information Security Standard (SEC501)
  - Introduces minimal amount of new requirements
- Aligns with security controls and best practices included in federal information security standards
  - National Institute of Standards and Technology (NIST 800-53)

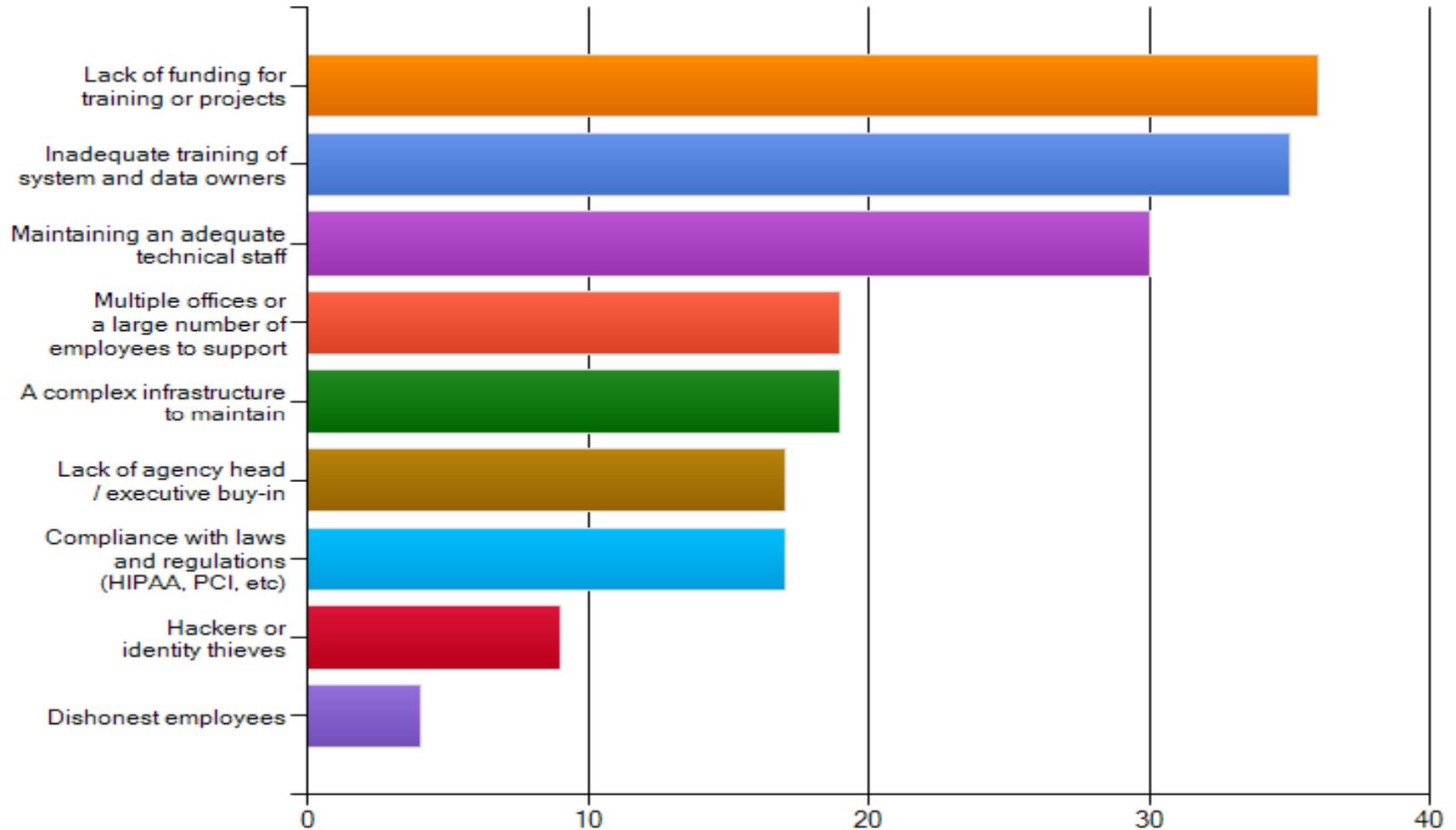


## Primary Drivers of the Restructuring

- Federal data and federally funded programs typically require compliance with NIST
  - FTI, SSA, etc.
- More efficient alignment with other security frameworks
  - ISO27001/ISO27002, HIPAA, COBIT, etc
- Enables direct comparison to private industry and other government entities
- Better integration with information security tools
- Leverage existing complementary documentation



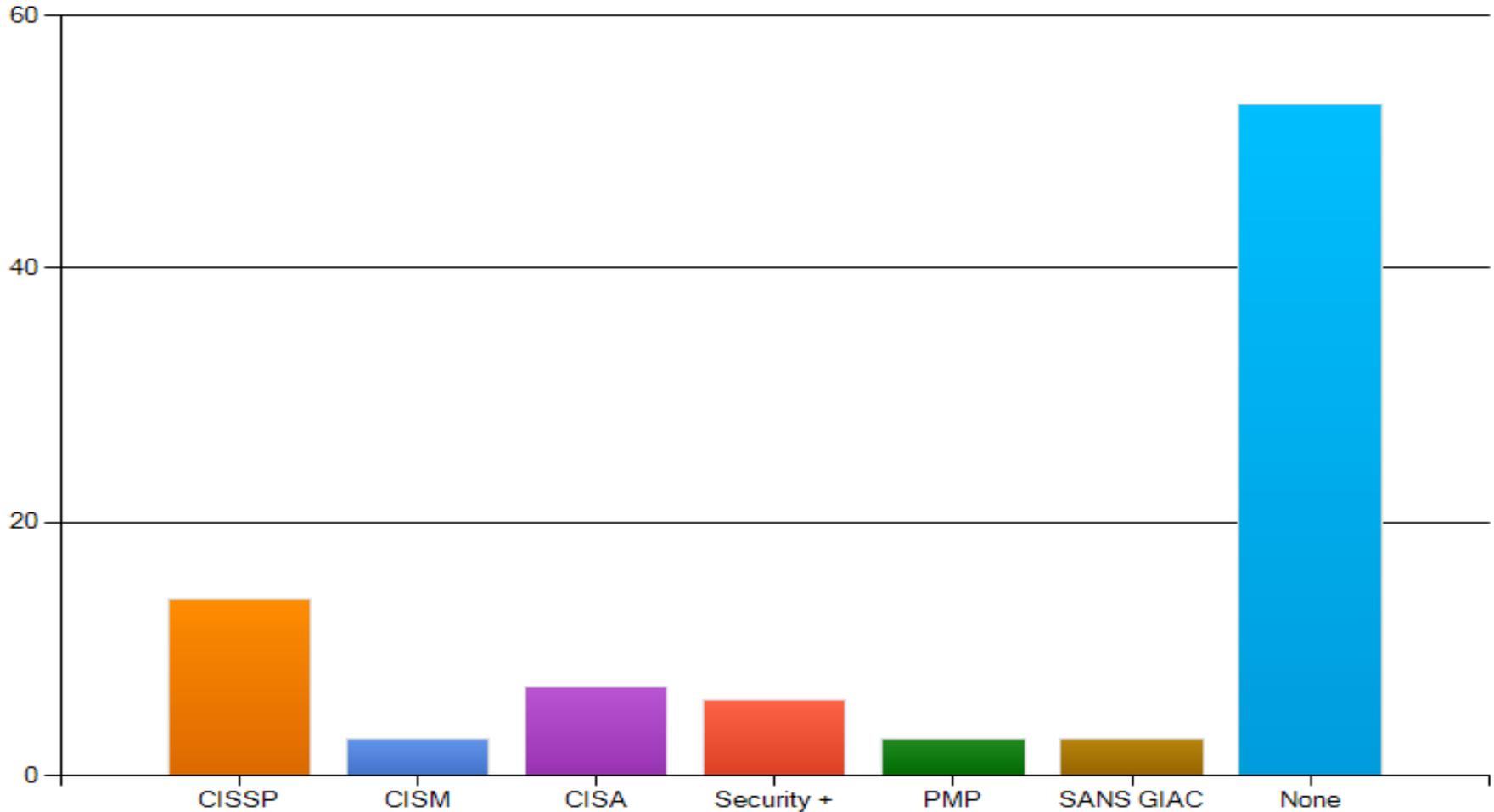
**What challenges do you feel are the most significant in terms of information security (select up to 3)?**



Source: Survey of security representatives from commonwealth agencies



What professional certifications do you currently hold and maintain (including vendor specific, e.g. Cisco, Redhat, Microsoft, etc.)?



Source: Survey of security representatives from commonwealth agencies



## Noteworthy Changes

- Information Security Officer Certification Program
  - Response to lack of agency emphasis on information security expertise in the agency
- Requires analysis and documentation of resources used for information security



## Impact to Agencies

- Minimal agency impact
  - No significant fiscal impact expected
- More efficient evaluation of agency information security program
  - Better comparison of agency information security programs



## Summary

- Restructured SEC501 to align with common information security framework
  - Meets federal requirements
  - More efficient
- Introduced information security officer certification program
- Require agencies document the information security resources they have chosen to make available
- Minimal fiscal impact to the agencies



Virginia Information Technologies Agency



# Questions?

