Security Architecture Report:

"A Security Framework for Delivering Business Solutions"

Version 1.0, May 2001

Prepared for:
The Council on Technology Services
Commonwealth of Virginia

By:
The COTS-Enterprise Architecture Workgroup,
Security Domain Team

Security Domain Team Members

Tim Bass (Co-Chair)	Virginia Retirement Services
Randy Horton (Co-Chair)	Department of Rehabilitation Services
Craig Drain	Department of Taxation
Rick Fowler	Department of Social Services
Don Kendrick	Department of Motor Vehicles
Jim Magill	Fairfax County Government
Art Phaup	Department of Information Technology
Ron Secrest	George Mason University
Mick Vollmer	City of Virginia Beach

Domain Support Staff

Paul Lubic	Department of Technology Planning, Manager
Brian Mason	Department of Technology Planning
Diane Wresinski	Department of Technology Planning
Paul Bucher	Virginia Department of Transportation

COTS Enterprise Architecture Workgroup

David Molchany, Co-Chair	Fairfax County, Local Government Representation
Murali Rao, Co-Chair	Department of Transportation, Secretariat of Transportation Representation
Tim Bass	Virginia Retirement System, Independent Agency Representative
Bethann Canada	Department of Education, Secretariat of Education Representative
Troy DeLung,	Department of Environmental Quality, Secretariat of Natural Resources Representative
Linda Foster	Department of Taxation, Secretariat of Finance Representative
Bob Haugh	Department of Corrections, Secretariat of Public Safety & Large Agency Representative
Randy Horton	Department of Rehabilitative Services, Secretariat of Health and Human Services Representative
James Jokl	University of Virginia, Higher Education Representative (UVA)
Ted McCormack	Commission on Local Government, Secretariat of Administration & Small Agency Representative
Bill Mize	Department of Information Technology, Secretariat of Technology Representative
Bob Pontius	Employment Commission, Secretariat of Commerce and Trade Representative

Table of Contents

EXECUTIVE SUMMARY....4
I. MISSION....7
II. INTRODUCTION AND BACKGROUND....7
III. METHODOLOGY....8
IV. PRINCIPLES....9
V. SECURITY COMPONENTS....11
A. BUSINESS ANALYSIS AND RISK ASSESSMENT....12
A.1 Standards....12
A.2 Best Practices....13
B. SECURITY AWARENESS....14
B.1 Standards....14
B.2 Best Practices....15
C. TECHNICAL TRAINING....15
C.1 Standards....16
C.2 Best Practices....16
D. TECHNICAL COMMUNICATIONS....16
D.1 Standards....16
D.2 Best Practices....17
E. AUTHENTICATION, AUTHORIZATION AND ENCRYPTION....17
E.1 Standards....18
E.2 Best Practices....19
F. DATA SECURITY....20
F.1 Standards....20
F.2 Best Practices....20
G. SYSTEMS INTEROPERABILITY SECURITY....21
G.1 Standards....22
G.2 Best Practices....22
H. PHYSICAL SECURITY....23
H.1 Standards....23
H.2 Best Practices....24
I. PERSONNEL SECURITY....24
I.1 Standards....25
I.2 Best Practices....25
J. THREAT DETECTION....25
J.1 Standards....26
J.2 Best Practices....26
K. SECURITY TOOL KIT....27
K.1 Standards....27
K.2 Best Practices....27
L. INCIDENT HANDLING....28
L.1 Standards....28
L.2 Best Practices....28
M. AUDITING SYSTEM ACTIVITIES....29
M.1 Standards....29
M.2 Best Practices....29

APPENDIX A: "EA COMMON REQUIREMENTS VISION" IMPLICATIONS 30
APPENDIX B: RELATED WEBSITES AND REFERENCES 33
APPENDIX C: GLOSSARY & ACRONYMS 33
GLOSSARY: ***34***
ACRONYMS: ***36***
APPENDIX D: SUMMARY LIST OF STANDARDS BY COMPONENT 37
APPENDIX E: SUMMARY LIST OF BEST PRACTICES BY COMPONENT 41

Executive Summary

The ***Security Architecture*** is an integral and critical domain within the Enterprise Architecture designed specifically to:

- enable secure communications and the appropriate protection of information resources within the Commonwealth;
- support the legal information security requirements established by existing Federal and State statutes pertaining to information confidentiality, accessibility, availability, and integrity;
- support secure, efficient transaction of business and delivery of services; and
- leverage opportunities to obtain I.T. security synergies and economies of scale.

Accordingly, the Security Architecture supports the overarching goal of ***Enterprise Architecture*** to enable and accelerate the development of the "Digital Dominion" by providing a consistent framework that aligns information technology resources with business strategies, and that fosters effective and timely technical decision-making.

The relative significance of the Security Architecture is highlighted by observing current trends in both technology uses and abuses. For example, the number of DNS hosts on the Internet grew from approximately 30 million in 1998 to 110 million in 2001[1]. Over that same time frame, the Federally-sponsored Computer Emergency Response Team (CERT) reported a ten-fold increase in security incidents[2]; while information compiled from the FBI and Computer Security Institute[3] indicate that:

- 90% of organizations detect some form of information technology security breach;
- 70% of information technology security breaches involve theft of information, financial fraud, or the sabotage of networks or data;
- 71% of organizations experience attacks from insiders, and 59% via the Internet;
- computer based financial fraud results in $1 million in losses on average.

Three external market factors currently fuel these national trends:

- latent and immature I.T. security policy, law and industry standards;
- a shortage of personnel with security technology expertise and experience; and
- engineering for "ease of use" has not been matched by engineering for "ease of security".

The attached Security Architecture, as developed by the Security Domain Team, is a ***foundational guidance document*** for addressing these security challenges and technology opportunities, while pursuing the Commonwealth's business mission. It provides a framework for ***consistency, coordination, and collaboration*** in applying security safeguards across the Agencies of the Commonwealth. At the same time, it provides Agencies the latitude to use risk-based decision-making processes to determine the

[1] "Internet Domain Survey", Internet Software Consortium, January 2001, http://www.isc.org/ds/
[2] "CERT Statistics, 1988-2000", Software Engineering Institute, http://www.cert.org/stats/cert_stats.html
[3] "Internet Security Trends", Rich Pethia, Carnegie Mellon University, February 2001, http://www.cert.org/present/internet-security-trends/index.htm

appropriate level of protection and product types to be used for obtaining compliance to Security policies. The Security Architecture is segmented into thirteen distinct components (e.g., Data Security, Physical Security, Intrusion Detection, etc.). However, each component is not mutually exclusive, i.e., the components are interdependent. Accordingly, the Security Domain Team recommends approval of the Security Architecture, Version 1.0, as a whole.

Implementation of the Security Architecture, Version 1.0, would require the following actions:

1. The formulation and promulgation of ITRM Policies, Standards and Guidelines (PSGs) by the Department of Technology Planning (DTP) that capture the standards and best practices which are outlined in Section V of the Security Architecture. [This would supersede COV-ITRM Standard SEC2000-01.1.]
2. The on-going development and administration of Security Programs by Agencies as directed by the PSG's.
3. The review of Agency Procurement Requests (APR's) submitted by Agencies for compliance to ITRM Security standards or a planned migration path towards said standards.
4. The creation and staffing of a centralized ***Security Center of Excellence*** under the direction of the Secretary of Technology (*Code of Virginia § 2.1-51.45*) which would provide the following services to Agencies:

Service Name	***Description***
Incident Response	Establish a network of specialists to assist Agencies contain, eradicate, and recover from security attacks. This team would include staff as well as non-staff members who agree to be "on-call".
Announcements/Alerts	Serve as the focal point for disseminating statewide alerts regarding security threats, active attacks, protective measures, and incident status.
Technology Watch	Stay abreast of new technology and services; and assess, summarize, and report their security impact and value to all Agencies.
Security Consulting	Provide expert advice to Agencies as needed regarding computer security issues for design, development, procurement or operations.
Best Practices	Stay abreast of new standards, methods, and applications in the industry; and assess, summarize and report successes and best practices to all Agencies.
Security Training	Offer training opportunities to Agencies to assist them develop their skills sets in such areas as risk assessment, safeguard implementation, incident detection, etc.
Procurement Contracts	Ascertain the need for state-wide procurement contracts for security products or services, and assess when economies of scale could be achieved.
Collaboration	Establish collaborative relationships with other entities such as law enforcement, public affairs, and service providers for rapid response to security issues.
Coordination	Facilitate interactions with both internal and external parties during implementation of security architecture, shared Agency projects, and public key infrastructure; and resolve interoperability issues.

The Security Domain Team strongly feels that these actions and related services best position the Commonwealth to:

- promote the ease and quality of security engineering across the enterprise;
- leverage the State's limited resource pool and budgets;
- prevent fragmentation when applying security technology and practices within Agencies;
- allow for the rapid response to both technology opportunities and to security threats; and
- enable the Commonwealth to take advantage of, adjust to, and/or influence the direction of industry security practices, standards, technology, and legislation.

I. Mission

The mission of the Commonwealth of Virginia's Security Architecture is to provide a framework to enable secure communications and the appropriate protection of information resources within the Commonwealth. This architecture must support the legal requirements established by existing Federal and State statutes pertaining to confidentiality, accessibility, availability, and integrity. Within this context, it must also support the efficient transaction of business, delivery of services, and communications with the Public, Agencies, businesses, localities, educational institutions, and other governmental bodies. And lastly, it must position the State to be able to quickly respond to technology, business, and information requirements changes without compromising the security, integrity, and performance of the enterprise and its information resources.

II. Introduction and Background

Introduction

The Commonwealth's Security Architecture consists of a set of security components that represent the framework for achieving the Mission stated above. Each security component is made up of common services and technologies. The Security Domain team identified the following 13 components as comprising the current Commonwealth of Virginia Security Architecture:

- Business Analysis and Risk Assessment
- Security Awareness
- Technical Training
- Technical Communications
- Authentication, Authorization and Encryption
- Data Security
- Systems Interoperability Security
- Physical Security
- Personnel Security
- Threat Detection
- Security Tool Kit
- Incident Handling
- Auditing System Activities

For each of these components, a set of security standards and best practices are defined by the security architecture. (See Section V, Domain Components.)

In this manner, ***the Security Architecture supports and promotes the consistent and effective development and implementation of Security programs by the State's Agencies and across the enterprise.***

Background

The following excerpt from the Commonwealth of Virginia "Information Technology Security Policy (COV-ITRM Policy 90-1)" reflects the driving business need for security architecture:

> "The Commonwealth relies heavily on the application of information technology for the effective management of governmental programs. Rapid and continuing technical advances have increased the dependence of State Agencies on information systems. The value of State information, software, hardware, telecommunications, and facilities must be recognized by Agencies as an important State resource, and be protected through Agency security programs.
>
> It is the policy of the Commonwealth that each Agency head is responsible for the security of the Agency's information technology resources and that all State Agencies shall take appropriate steps to secure their information technology resources and sensitive information through the development of an Agency information technology security program. As security encompasses a broad spectrum of safeguards, each Agency should determine which information resources must be protected. All systems must include security safeguards that reflect the true importance of the information processed on the system and/or the State's investment embodied in the components of the information technology system.
>
> The specific structure of an Agency's information technology security program will vary depending on the scope and nature of the information technology resources and sensitive information for which the Agency is responsible."

III. Methodology

The development of Domain architecture is part of the overall Enterprise Architecture Process Model utilized used by the Commonwealth of Virginia. The development of an enterprise-level "Common Requirements Vision" and "Conceptual Architecture" were prerequisites to this step in the EA Process Model. (The EA Process Model and related deliverables are documented at http://www.sotech.state.va.us/cots/ea/eaabout.htm .)

The Security Domain Team conducted the following four activities as part of the "architecture modeling" of the security architecture:

- Validate the implications of the Technology Trends, Enterprise Business Strategies, and Requirements for Technical Architecture from the "EA Common Requirements Vision" on the Security Domain. (See Appendix A.)
- Validate the implications of the Conceptual Architecture Principles (CAP's) on the Security Domain; and, identify any specific domain principles that provide additional structure for the Security Architecture, or which further qualify or contextualize the CAP's from a security perspective. (See Section IV.)
- Identify and categorize the security services and technologies that will be governed by the domain, referred to as "security components". (See Section V)
- Identify and establish the standards and best practices for the "security components" of the security architecture. (See Section V)

IV. Principles

Security Domain Principles represent the fundamental concepts that provide the foundation for the standards, best practices, and configurations which compose the Security Architecture.

1) The Security Domain Team endorses and supports the Conceptual Architecture Principles (CAPs) identified by the COTS-EA Workgroup in the "EA Conceptual Architecture" document (http://www.sotech. state.va.us/cots/ea/eaconcep.htm), and deems them applicable to the Security Architecture ***as qualified*** in Item 2 below.

2) The Security Domain Team has further identified the following domain specific principles, which provide additional structure for the Security Architecture, and which further qualify and/or contextualize the CAP's from a security perspective.

   - The Security Architecture must facilitate proper and efficient security identification, authentication, authorization, administration and auditability in response to the access and use of information resources.

   - The Security Architecture must support and remain compliant with State laws and Federal regulations (e.g., H.I.P.A.A and Rehabilitation Act, Sec. 508) with respect to security, privacy, availability, accessibility, etc.

   - The Security Architecture must provide a modular approach to authentication, authorization, and accounting.

   - The Security Architecture must provide a common Open Authentication store.

   - The Security Architecture must provide for various strength Authentication models.

   - The Security Architecture must provide for portability across platforms.

   - The Security Architecture must utilize Open Standards at all modular levels.

   - The Security Architecture must support multiple service delivery channels where feasible.

   - The Security Architecture must ensure that security requirements and associated risks are adequately evaluated when preparing to support adaptability, availability, access, data capture and data sharing needs of the enterprise.

   - The Security Architecture must be flexible to support the introduction and/or integration of new technologies, while maintaining appropriate security protection and requirements.

- The Security Architecture must ensure that the accountability and responsibility of all persons fulfilling security duties are sustainable, assignable, and enforceable.

- The Security Architecture must address systemic needs as well as individual component needs.

- The Security Architecture must address and support multiple levels of protection, including network level, operating system, and application level security needs.

- The Security Architecture must support interfaces that can be utilized by other public and private entities wishing to participate in the Commonwealth's Security Domain.

- The Security Architecture must facilitate risk analysis, whereby the cost for security protection is appropriate to the level of security required.

V. Security Components

The following thirteen security components comprise the security technologies and services that form the security architecture.

- Business Analysis and Risk Assessment
- Security Awareness
- Technical Training
- Technical Communications
- Authentication, Authorization, and Encryption
- Data Security
- Systems Interoperability Security
- Physical Security
- Personnel Security
- Threat Detection
- Security Tool Kit
- Incident Handling
- Auditing System Activities

In this section, standards, implementation best practices and technology examples are outlined for the components above. The term "***standard***" means a directive or specification whose compliance by Agencies is mandatory, and whose implementation is deemed achievable, measurable, and auditable for compliance. The term "***best practice***" means a guideline or specification that is advisory in nature and whose compliance is strongly recommended; however, it is not binding on Agencies. Note, the standards and best practices will be drafted into COV-ITRM Policy, Standards, and Guidelines (PSG's) by the Department of Technology Planning, accordingly.

The term "***Agency***" means Commonwealth of Virginia executive branch Agencies and institutions of higher education. For the purpose of this document, however, any Academic "instruction or research" systems/infrastructure that can be isolated from "administrative and business" systems/infrastructure are considered exempt from the stated security architecture standards.

Concerning local governments and other public bodies, while they are not required to comply with the standards, the information technology specifications for participation in State programs would be based on the architecture described herein. This architecture was designed with participation of local government and other public body representatives with the intent of encouraging its use in State/Local interoperability activities.

A. Business Analysis and Risk Assessment

Business Analysis and Risk Assessment refer to those practices, technologies and/or services used to identify information resources that are confidential and/or critical to the Agency; and to identify and evaluate the potential security threats, and associated risks, to those resources.

The starting point of establishing effective information technology security is to identify the information resources that are owned and/or utilized by the Agency. "Information resources" include government information, information technology, and associated personnel (See Appendix C: Glossary). Once identified, the Agency needs to determine which of these resources require protection against unavailability, unauthorized access, or disclosure, i.e., their level of sensitivity. For example, various information may require protection under the Virginia Privacy Protection Act of 1976 or the federal Health Insurance Portability and Accountability Act (HIPAA); or, the unavailability of a database may adversely affect the ability of an Agency to accomplish its mission. This process is referred to as business analysis (or business impact analysis).

Once the level of sensitivity of the information resources has been identified through the business impact analysis, the threats to which they are subject need to be evaluated. This process is referred to as a risk assessment. The probability of each "threat event" occurring and the resultant impact of that event on the information resources are assessed during this process. Examples of potential impacts that would adversely affect the Agency and/or State include financial loss, public embarrassment, loss of public confidence, noncompliance to State or Federal statutes, and degraded customer (public) service. The Agency needs to decide if and when a residual level of risk may be acceptable.

Based on the business impact analysis and the risk assessment, the Agency determines what types of safeguards are appropriate to address their defined risks. In this manner, the safeguards deployed reflect the true importance of the State's investment in the information resources used to accomplish the Agency's mission. (Sections B through M address different types of security safeguards.) All implemented safeguards should be referable back to the business impact analysis and risk assessment.

Business impact analysis and risk assessment should not be viewed as just a one-time task or project, but rather as a tactical operational process. Both internal changes (e.g., changes to technical infrastructure or to applications) as well as external changes (e.g., technology advances, new Federal statutes, etc.) could directly impact the level of sensitivity and the threats applicable to information resources. Agencies, therefore, should intermittently deploy business impact analysis and risk assessment techniques to determine if their security safeguards are relevant and adequate, and then update their safeguards accordingly.

A.1 Standards

A.1.a) The head of each Agency shall be responsible for the security of the Agency's information resources; and formally appoints an Information Systems

Security Officer (ISSO) who is responsible for the development, implementation, oversight, and maintenance of the Agency's information security program.

A.1.b) Each Agency must establish, document, implement and maintain an information security policy and program appropriate to its business and technology environment. The policy and program must be consistent with Federal regulations (e.g., H.I.P.A.A; Rehabilitation Act Sec. 508) and State laws (e.g., Virginia Privacy Protection Act of 1976).

A.1.c) Security program documentation must specify how exceptions to security standards are to be handled. All such exceptions must be completely reviewed by a level of management above that approving the exception.

A.1.d) Each Agency must conduct a business impact analysis and risk assessment throughout the Agency (to include relevant business partners) to identify various levels of sensitivity associated with the information resources as defined; to identify the potential security threats to those resources; and to determine the appropriate level of security to be implemented to safeguard those resources. The business impact analysis and risk assessment can be reviewed and updated as needed, but at minimum must be reviewed and updated every three years.

A.1.e) Security programs must include protective measures and procedures to ensure that the appropriate levels of confidentiality, integrity and availability of data, information, and systems are sustainable.

A.1.f) Development, installation and/or changes to the Agency environment, technical infrastructure, and information systems must be reviewed for security implications and approved by the Agency's ISSO, or by person(s) delegated said approval authority by the Agency's ISSO, as part of the planning and design process; and then coordinated thoroughly during development and implementation. Acknowledgement of this review and approval by the Agency's ISSO, or delegated authority, must be documented and auditable.

A.1.g) Security programs must be coordinated and integrated with contingency planning and business resumption activities.

A.2 Best Practices

A.2.a) In assigning the level of risk, each Agency should evaluate both the probability of an event occurring and the resultant effect of that event on the confidentially, availability, and integrity of system components and data.

B. Security Awareness

Security Awareness refers to those practices, technologies and/or services used to promote User awareness, User training and User responsibility with regards to security risks, vulnerabilities, methods, and procedures related to information technology resources. A "User" is an individual or group who has access to an information system and/or its data (See Appendix C: Glossary).

Users within an Agency need to understand the sensitivity of the Agency's information resources (discussed in Section A) and their responsibility in protecting those resources. For example, Users should be aware of the threats and the associated impacts of a compromised password; of potential viruses transmitted over the Internet; of corrupted databases; and of the accessibility of printed information generated from the system.

Although, responsibility to adhere to State statutes and Agency policy and procedures are accepted by personnel upon engagement, Security Awareness programs provide a proactive mechanism to foster further comprehension of an individual's security responsibilities; to contextualize security responsibilities to specific job duties and case examples; to motivate personnel towards a security-conscious behavior while performing their duties; and to reinforce the consequences of security failures on the State, the Agency, its mission, its customers, and the User.

The appropriate amount, depth, and timing of Security Awareness is a risk-based decision. Best practices suggest that a Security Awareness program that utilizes a combination of periodic training sessions (introductory/refresher) and on-going security awareness promotion (marketing) are most effective. In addition, where appropriate, an Agency may decide not to grant certain access rights to personnel until the desired level of Security Awareness Training has been successfully completed. Lastly, as the business and technical environment changes, security awareness material will need to be updated accordingly.

B.1 Standards

B.1.a) Each Agency must establish and maintain information technology security awareness programs to ensure that all individuals are aware of their security responsibilities and know how to fulfill them.

B.1.b) A security awareness training program must:

- be approved by the Agency's Information Systems Security Officer (ISSO);
- specify timeframes for receiving training (initial, ongoing and/or refresher);
- provide both general and position appropriate security awareness content; and
- be documented on an auditable medium.

B.1.c) All new hires must receive formal security awareness training as designed by their Agency within 30 calendar days of their start date.

B.1.d) Receipt of Security Awareness Training must be documented in the employee's personnel file with employee's acknowledgement of receipt and understanding.

B.1.e) Security Awareness Refresher Training must be provided to personnel annually at a minimum.

B.2 Best Practices

B.2.a) Security Awareness programs should contain content that covers, but is not limited to:

- Responsibility of users to report issues;
- Users can be audited;
- Legal requirements for data (citing legislation as appropriate);
- Privacy expectations;
- Ownership of data;
- Acceptable use policy for E-mail and Internet Browsers; and
- Sensitivity to threats, risks, vulnerabilities.

B.2.b) Security Awareness programs should include a means to promote security awareness on an on-going basis, i.e., supplemental to training (e.g., security awareness banners, posters, "security day", etc.)

B.2.c) Security Awareness training content is not static, and should be continuously reviewed and updated by each Agency as needed to reflect changes to the Agency's environment, business, technology, systems and information.

C. Technical Training

Technical Training refers to those practices, technologies and/or services used in training Security officers, system administrators and/or other personnel involved in the administration or development of information systems.

Individuals who are assigned responsibilities for information technology security safeguards need in-depth training regarding the security methodologies and techniques required to configure, implement, administer, and maintain those safeguards. For example, a security administrator may need to know the method and techniques for granting various types of access rights to the database, how to set up and maintain an effective firewall to filter external access, and how to detect intrusions to the system. Typical sources for technical training include instructor-led programs (3rd party or internal), commercial off-the-shelf training modules, technical publications, and operations manuals provided by the vendor.

C.1 Standards

C.1.a) Each Agency must establish and maintain information technology security training programs to ensure that all individuals involved in managing, administering, designing, developing, implementing, and/or maintaining information resources are aware of their security responsibilities and know how to fulfill them.

C.1.b) Information technology security training programs must be commensurate to the level of expertise required for the system components and information resources for which they are responsible. The program must include content that enables the individual to identify and evaluate threats, vulnerabilities, and risks specific to those components and resources. The program must further include content regarding technical alternatives, methods, and standards which represent best practices appropriate to those components and resources, and which can be utilized to effectively implement safeguards as appropriate.

C.2 Best Practices

C.2.a) Each Agency should consider using certification programs to promote high-level, up-to-date technical security expertise (e.g., CISA, CISSP or SANS).

D. Technical Communications

Technical communications refer to those practices, technologies and/or services used to communicate technical information and notifications regarding the status of security related events and safeguards.

In addition to the communications inherent in Security Awareness and Technical Training, the security architecture requires a means to support the timely and meaningful exchange of information regarding: 1) new security technology products and/or features, best practices, emerging industry standards, and security safeguards success stories; 2) proposed changes to the security infrastructure and associated implementation plans; and 3) alerts, status, and recommended actions in response to security attacks. Examples of technical communication medium include internal enterprise list servers, government sponsored security conferences, subscriptions to security research consortiums, etc.

Technical communications are instrumental in the security architecture as they foster both a proactive stance and a systemic view in addressing security issues within a dynamic business and technology environment.

D.1 Standards

D.1.a) Each Agency must subscribe to the technical security dissemination service(s) provided by the state's Security Center of Excellence. Each Agency must disseminate information received through the above service(s) to the appropriate personnel within their organization in a timely manner.

D.1.b) If any data or documentation contains sensitive information, then the Agency must ensure that such information is given accountable and authorized dissemination only.

D.2 Best Practices

D.2.a) Each Agency should subscribe to industry and vendor security mailing lists for the appropriate system components used within, or interfaced by, the Agency.

D.2.b) Organizations should consider and encourage including information security topics in conferences, symposia, seminars, etc., where appropriate (e.g., the Commonwealth of Virginia Information Technology Symposium (COVITS)).

E. Authentication, Authorization and Encryption

Authentication refers to the process of verifying the identity of a user. Authorization refers to the process of establishing and enforcing a user's rights and privileges to access specified resources. Encryption refers to the process of converting computer data and messages to something incomprehensible by means of a key, so that it can be reconverted only by an authorized recipient holding the matching key.

Authentication answers the question, "Are you who you say you are?" It is a means of establishing the validity of a claimed identity to the system, which becomes the basis for individual accountability. There are three means of authenticating a user's identity, which can be used alone or in combination: 1) validating something the individual knows (e.g., a password, a Personal Identification Number (PIN), or a cryptographic key); 2) validating something the individual possesses, referred to as a "token" (e.g., an ATM card or a smart card); or 3) validating something the individual "is", referred to as a "biometric" (e.g., fingerprints or voice patterns).

Once authenticated, logical access controls are utilized to authorize and enforce a user's access to and actions towards specified resources. This authorization may be based on identity, roles (e.g., data entry clerk, administrator, supervisor) location, time, types of transactions, service constraints (e.g., number of concurrent users), access mode (e.g., read, write, delete), or a combination of these criteria. Both internal authorization safeguards (such as Access Control Lists) and external controls (such as secure gateways/firewalls) can be deployed. Another mechanism that can be used for strong access control is encryption, whereby encrypted information can only be decrypted by those possessing the appropriate cryptographic key. Figure 1 (below) provides guidance regarding the major industry algorithms used in support of encryption.

Figure 1: Cryptographic Algorithms
(The terms "Obsolescent, Transitional, Strategic, and Emerging" are defined in the Glossary in Appendix C.)

Obsolescent	Transitional	Strategic	Emerging
Public Key: Rivest-Chor Merkle-Hellman	**Public Key:** Rabin Diffie-Hellman ElGamal LUC (Lucas sequences)	**Public Key:** RSA (Rivest-Shamir-Adleman) DSS (Digital Signature Standard) ECC (Elliptic Curve Cryptosystem)	**Public Key:** XTR (Efficient Compact Subgroup Trace Representation) NTRU
Secret Key: RC2	**Secret Key:** OTP (One Time Pad) DES (Digital Encryption Standard) RC4	**Secret Key:** 3DES (Triple Digital Encryption Standard) IDEA (International Data Encryption Algorithm) Blowfish	**Secret Key:** AES (Advanced Encryption Standard) Twofish MARS RC6 Serpent
Hash Functions: MD2 (Message Digest 2) MD4 (Message Digest 4)	**Hash Functions:** MD5 (Message Digest 5)	**Hash Functions:** SHA-1 (Secure Hash Algorithm)	**Hash Functions:** RIPEMD-160 (Race Integrity Primitives Evaluation Message Digest)

E.1 Standards

E.1.a) Each Agency must ensure that Users are authenticated prior to accessing the systems which are "owned" by that Agency.

E.1.b) Each Agency must establish a formal authentication control policy that establishes the criteria for administering authentication safeguards.(e.g., a formal password policy that includes the criteria for password aging, history, length and composition).

E.1.c) Each Agency must store all sensitive data used in authenticating the user, including passwords, in protected files.

E.1.d) Public key certificates must be based on the most current IETF X509 standards.

E.1.e) Each Agency must authorize based on least privilege. Least privilege states that a user is given only that set of privileges necessary to perform his/her job.

E.1.f) The use of cryptology technologies for data storage and data communications (transmission of data) must be based on open standards.

E.1.g) All Virginia On-Line Transaction (VOLT) Certificates utilized by an Agency must be issued by service providers who are currently granted "Authorized Certificate Authority" status via a Virginia VOLT contract.

E.2 Best Practices

E.2.a) Each Agency should identify a method of verifying user authenticity on a spectrum from "null/weak" to "strong" authentication methods. Authentication is based on validating the following three criteria presented by the user: 1) "What do you know?", 2) "What do you have?", and 3) "Who are you?". Weak authentication is based on validating one of these criteria only, and should only be used when a minimum level of authentication is desired. Strong authentication, which is based on validating two or more of the criteria, should be used in all other cases.

E.2.b) Each Agency should establish policy and procedures that address when different levels of encryption, digital signatures, and digital certificates are appropriately used.

E.2.c) Digital signature and digital certificate technology can be used by Agencies to verify the authenticity of electronically transmitted data. If high-assurance digital certificates are deemed appropriate, Agencies should use either Virginia On-Line Transaction (VOLT) Certificates, or high-assurance certificates that are compatible with VOLT Certificates.

E.2.d) With regards to Digital Signatures, Agencies should use the VOLT Public Key Infrastructure wherever possible, and should adhere to the Internal Control and Auditing practices established to support the use of digital certificates in the Commonwealth.

E.2.e) Each Agency should establish Encryption Key Management policy and procedures to address the integrity and recovery of the "keys".

E.2.f) Each Agency should identify criteria governing the number of unsuccessful login attempts allowed by a user, and the resetting of passwords.

E.2.g) Authorization should use role-based access models.

E.2.h) Each Agency should use single sign-on technology where appropriate**.**

E.2.i) Each Agency should strongly consider encryption to protect sensitive data, including passwords, that are transmitted over a public network (e.g., replace Telnet with SSH).

E.2.j) Each Agency should strongly consider encryption to protect sensitive data, including passwords, transmitted over an internal network.

F. Data Security

Data Security refers to those practices, technologies and/or services used to ensure that security safeguards are applied appropriately to data which is provided, processed, exchanged and/or stored by the State.

The term "data" includes, but is not limited to, data in a database, information about an Operating System (OS), operational policies and procedures, system design, organization policies and procedures, system status, and personnel schedules. Data Security safeguards strive to sustain the level of integrity, availability and confidentiality of this data as stated by the Agency's policy. Data security is the responsibility of the data owner. The appropriate types/pieces of data (procedures, databases, operating documents, etc) and their level of sensitivity should be identified as part of the business impact analysis and risk assessment (see Section A).

Examples of data security safeguards include Agency developed procedures (e.g., information distribution and change management procedures), vendor delivered configurable controls (e.g., automatic screen savers), and add-on technologies (e.g., hashing algorithms). Data security safeguards are clearly interdependent with other safeguards described in this architecture (e.g., physical security, authentication, authorization, and encryption).

F.1 Standards

F.1.a) Ownership of data must be specifically identified by each Agency. [Note, based on the Agency's business impact analysis and risk assessment referred to in Section A, files and data elements to be protected will be identified.]

F.1.b) Owners are responsible for determining the appropriate levels of data security required.

F.1.c) All sensitive data must be removed from system hardware, software or media by the owner prior to its "reuse" by another Agency, or for "reuse" by another system within the Agency. Similarly, all sensitive data must be removed from system hardware, software or media by the owner prior to its disposal.

F.2 Best Practices

F.2.a) Desktop platforms, including laptops, should have a protected screen saver mechanism, which is activated.

F.2.b) Automatic protected screen savers should be initiated by the system after a specific period of inactivity.

F.2.c) Auditable user agreements should be utilized to delegate responsibility for data security from data owners to data custodians. Custodians are responsible for ensuring that the levels of required protection are followed.

G. Systems Interoperability Security

Systems interoperability refers to those practices, technologies and/or services used to ensure that security safeguards are applied consistently and appropriately to mechanisms that allow diverse systems and networks to interoperate.

Agencies often depend on interoperability for the timely exchange and sharing of information and data to effectively perform their business services. An Agency's systems may interoperate with those of other Agencies, other governmental bodies (local, state, or federal), with businesses or with public users; and those systems may operate on different platforms or with different technologies. Synergies, cost savings, and economies of scale can result by ensuring that security safeguards between "interoperating entities" are compatible and sustain the desired security protection levels of those entities. Industry best practices suggest that deploying vendor-neutral, open standards provides a common denominator in support of interoperability. Figure 2 (below) provides guidance regarding widely accepted industry security protocols.

Figure 2: Widely Accepted Security Protocols

(The terms "Obsolescent, Transitional, Strategic, and Emerging" as defined in the Glossary in Appendix C.)

Security Protocol for:	Obsolescent	Transitional	Strategic	Emerging
WWW connections			SSL/TLS (Secure Socket Layer/Transport Layer Security)	SHTTP (Secure Hypertext Transfer Protocol)
E-mail Security			Open PGP (Pretty Good Privacy) Secure MIME (Multi-purpose Internal Mail Extension)	
Terminal sessions & TCP connections.		SSH1 (Secure Shell)	SSH2 (Secure Shell)	
Distributed Name Services				DNSSEC (Domain Name Server Security)
API to cryptographic algorithms				GSSAPI (Generic Security Services API)
Network Tunneling		PPTP (Point to Point Tunneling) L2F (Layer Two Forwarding)	IPSec (Internet Protocol Security) L2TP (Layer Two Tunneling Protocol)	
Key Exchange			SKIP (Simple Key Management for Internet Protocol)	ISAKMP (Internet Security Association Key Management Protocol)

G.1 Standards

G.1.a) Each Agency must ensure that authentication, authorization and data security, as established by the data owner, is not compromised during data sharing and systems interoperability.

G.1.b) Auditable user agreements must be established between the Agencies sharing data, which clearly state the degree of authentication and levels of protection required.

G.1.c) Web-enabled transactions that require user authentication, or transfer of sensitive data, or that involve the transfer of funds, must use encryption (e.g. SSLv3).

G.2 Best Practices

G.2.a) Agencies should use open standard-based security solutions, as opposed to unique generated security solutions, to support current interoperability needs and to position them for future interoperability needs.

G.2.b) Agencies should use open standard based encryption algorithms when sharing sensitive data internally; and externally for data that requires encryption that is resident on that system.

G.2.c) New deployments of VPN (Virtual Private Network) technologies should use IPSec (Internet Protocol Security).

G.2.d) E-mail should not be considered a secure transport in itself. Therefore, any attachment containing sensitive information should be encrypted (e.g., using Pretty Good Privacy (PGP)).

G.2.e) Unencrypted Telnet, FTP, or R-Utilities should not be used.

G.2.f) Secure Shell Protocol (SSH) and Secure Hypertext Transfer Protocol (SHTTP) should be deployed for remote terminal sessions and file transfers.

G.2.g) 40 bit encryption should be used with SSL transactions to ensure global interoperability unless there is a requirement to use a higher bit encryption. (E.g. Virginia Militia or Virginia citizens residing overseas may be limited to 40 bit encryption.)

G.2.h) 1024 bit key digital server certificates should be used for SSL.

G.2.i) Agencies using digital certificates should seek interoperability with those digital certificates utilized by other government bodies(Federal, State, and Local). Virginia On-Line Transaction (VOLT) Certificates are designed for such compatibility.

H. Physical Security

Physical Security refers to those practices, technologies and/or services used to ensure that physical security safeguards are applied. Physical security safeguards take into account 1) the physical facility housing the information resources; 2) the general operating location; and 3) the support facilities that underpin the operation of the information systems.

Accordingly, physical security safeguards need to be considered for information resources residing in static facilities (such as buildings), mobile facilities (such as computers mounted in vehicles), and portable facilities (in-transit facility housing). Appropriate physical safeguards need to be established based on the risks related to geographic location, including natural threats (such as flooding), man-made threats (such as burglary or civil disorders), and threats from nearby activities (such as toxic chemical processing or electromagnetic interference). Lastly, physical safeguards need to assure that the appropriate levels of support facilities such as electric power, heating, and air-conditioning are sustainable as required by the information resources.

For example, physical access controls may be used to restrict and monitor the entry and exit of personnel to/from a room, a data center, or a building. Physical access controls may range from badges and locks to retina scanning personal identification devices and vibration detectors. Physical access controls should be considered for those areas containing system hardware, as well as for those areas which house network wiring, electric power, backup media, source documents, etc.

Physical security safeguards provide a first line of defense for information resources against physical damage, physical theft, unauthorized disclosure of information, loss of control over system integrity, and interruption to computer services.

H.1 Standards

H.1.a) Mission critical system facilities must be located in a secure location that is locked and restricted to authorized personnel only.

H.1.b) Access to "critical" computer hardware, wiring, displays and networks must be controlled by rules of least privilege.

H.1.c) System configurations (i.e., hardware, wiring, displays, networks) of "critical" systems must be documented. Installations and changes to those physical configurations must be governed by a formal change management process.

H.1.d) A system of monitoring and auditing physical access to "critical" computer hardware, wiring, displays and networks must be implemented (e.g. badges, cameras, access logs).

H.1.e) Back-ups of mission critical data must be stored off-site in a secured location.

H.2 Best Practices

H.2.a) Mission critical system components should be located in an environmentally friendly area (e.g., which includes fire protection, HVAC, UPS).

H.2.b) Access to computer hardware, wiring, displays and network should be controlled by rules of least privilege.

H.2.c) System configurations (i.e., hardware, wiring, displays, network) should be documented. Installations and changes to those physical configurations should be governed by a formal change management process.

H.2.d) Physical Access security for back-up systems should be equivalent to that of the primary facilities.

H.2.e) A system of monitoring and auditing physical access to computer hardware, wiring, displays and networks should be implemented (e.g., badges, cameras, access logs).

I. Personnel Security

Personnel Security refers to those practices, technologies and/or services used to ensure that personnel security safeguards are applied appropriately to those personnel working for, or on behalf, of the State.

Personnel Security begins during the Staffing process. Early in the process of defining a position, the responsible supervisor determines the type of computer access that is needed for the position and the sensitivity of that position. Best practices suggest that two general principles should be followed in defining a position: *separation of duties* and *least privilege*. Separation of duties refers to dividing roles and responsibilities so that a single individual cannot subvert a critical process. For example, separate responsibility should be given for requesting a personal identification number and for authorizing a personal identification number. Least privilege refers to granting a user only those accesses that they need to perform their official duties. For example, a data entry clerk may not need to run analysis reports against the entire Agency database. As part of the process to fill a position, best practices also suggest that testing and background screening should be used as appropriate to help validate and/or access a candidate's qualifications, past performance and appropriateness for a particular position.

Once personnel have been staffed, personnel security safeguards are administered according to the Agency's security policy via User account management. User account management involves 1) establishing the procedures for requesting, issuing, and closing user accounts over the life cycle events of personnel (e.g., initial hire, transfers, position

promotion, retirement, resignation, etc.); 2) tracking users and their respective access authorizations; and 3) managing these functions on an on-going basis.

I.1 Standards

I.1.a) Access must be explicitly granted to personnel by the Owner (i.e., not allowed by default).

I.1.b) Access granted to personnel must be based on least privilege (i.e., only up to the level needed to perform one's duties).

I.1.c) Access must be terminated concurrent with when the requirement for access no longer exists (e.g., as result of transfer, termination , and change of duties).

I.2 Best Practices

I.2.a) Each Agency should establish and document the process which directs the steps and the timing required to grant and withdraw physical and system access privileges to personnel for the following events: new hire, employee transfer to another Agency, employee termination, employee resignation, employee change of job duties within an Agency, and perceived disgruntled employee behavior. A similar process should be established for contractors (i.e., non-state personnel) working for or on behalf of an Agency.

I.2.b) System access should be granted via a formal and auditable process, and should be accompanied by security training which is commensurate to one's duties and responsibilities.

I.2.c) Non-Disclosure Agreements should be signed by all individuals who need access to "sensitive" information, prior to granting access to that information.

I.2.d) Background checks of personnel may be required consistent with Agency policy and depending on the sensitivity of information accessible to that position.

J. Threat Detection

Threat detection refers to those practices, technologies and/or services used 1) to detect that a suspicious activity may be occurring on systems/networks; and 2) to alert security administrators and security staff accordingly.

An attack on a system or network can come from either inside or outside of an Agency, and could be intentional (e.g., transmittal of viruses, "worms", or "Trojan horses") or unintentional (e.g., accidental deletion of a control file).

Threat detection may include the real-time monitoring of activities such as logons, connectivity, operating system calls, command parameters, or system performance logs. Threat detection safeguards support the analysis of performance thresholds, behavioral anomalies, use patterns and trends (such as degradation in system performance over time), or the existence of known threats (such as known viruses). For example, automated tools could monitor the levels and rate of change in disk space on an E-mail server to determine if potential "spamming" (i.e., sending continuous bulk e-mail) is occurring with the potential to consume all available space on that server.

Threat detection may also include a review of activities "after the fact", and over a specific time frame (e.g., reviewing the number and types of rejected passwords overtime may indicate that a "password cracking" activity is under attempt.)

Alerts from automated threat detection tools may be active (immediate paging of appropriate security personnel) or passive (logging specific types of activities to a daily system security log for later review).

J.1 Standards

J.1.a) Each Agency must establish and implement a process to identify and evaluate threats and assign appropriate action based on risks.

J.1.b) Firewall technology must have security logging turned on.

J.2 Best Practices

J.2.a) Violations of those parameters set in conjunction with the Agency's threat detection program should trigger an appropriate form of security notification to security administrators or security staff.

J.2.b) Systems should be designed to handle both passive and active alarms.

J.2.c) A security event log should be kept for each device. These logs should be analyzed, correlated and evaluated to identify and respond to suspicious activity.

J.2.d) Security logs should be archived on a daily basis.

J.2.e) Security logs should be moved off the device as soon as possible and stored on an off-site location.

J.2.f) Intrusion detection systems should be deployed both externally and internally to the firewall technology protecting the network.

J.2.g) Agencies should get assistance from the Computer Incident Response Team (CIRT) provided by the state's Security Center of Excellence as needed to trouble shoot unusual or "difficult to isolate" threats.

K. Security Tool Kit

This section refers to those practices, technologies and/or services used to manage, analyze, filter, test and/or control security safeguards. For example, firewall technology provides a mechanism through which authentication, authorization, filtering and directing of remote users to an internal system can be accommodated. Typically an Agency's security tool kit will be comprised of a combination of commercial off-the shelf products, industry proven free shareware, and Agency developed software tools. The tools may be positioned on the perimeter of systems or integrated into the systems; and may be deployed on either an operational or as needed basis. Examples of common technologies within an organization's security tool kit include firewall technology, vulnerability scanners, and sniffers.

K.1 Standards

K.1.a) Agencies with external connections using TCP/IP must utilize firewall technology.

K.1.b) Each Agency must test its firewall technology on a periodic basis to ensure compliance with security policies.

K.1.c) Each Agency must deploy multi-layered protection at the Internet gateway, the network server and the desktop levels to prevent the introduction of malicious code into the system.

K.2 Best Practices

K.2.a) Within the Agency, firewall technology should be implemented to protect sensitive internal information.

K.2.b) Each Agency should have the ability to monitor and capture traffic at any location within their network (e.g. via use of a portable sniffer).

K.2.c) Each Agency should use network and host vulnerability scanners to test for the vulnerabilities of internal systems and of perimeter defenses, and their adherence to security policy. Resulting vulnerabilities should be addressed.

K.2.d) Each Agency should scan all incoming e-mail for existence of malicious code (e.g., viruses), and contain and eradicate that code.

K.2.e) Each Agency should keep Virus signatures current by updating virus signatures weekly at a minimum.

L. Incident Handling

Incident Handling refers to those practices, technologies and/or services used to respond to suspected or known breaches to security safeguards.

Once a suspected intrusion activity has been qualified as a security breach (i.e., incident), it is imperative that the incident be contained as soon as possible, and then eradicated so that any damage and risk exposure to the Agency and the Commonwealth are avoided or minimized. Information technology security incidents refer to deliberate, malicious acts which may be technical (e.g., creation of viruses, system hacking) or non-technical (e.g., theft, property abuse, service disruption). In several cases, if the incident is left "unchecked" (i.e., not contained), then the damage resulting from these incidents continues to spread within, and across, Agencies.

Handling incidents can be logistically complex, and may require information and assistance from sources outside the Agency (e.g., technical specialists, law enforcement entities such as state police or FBI, and the public affairs office). Industry best practices suggest that organizations who adopt both proactive and reactive means to address incident handling are better able to limit the negative implications of incidents. Examples of proactive activities include establishing communication mechanisms to report incidents and to disseminate incident alerts; and identifying technical experts who can provide emergency assistance if needed. Examples of reactive activity include blocking or aborting computer processes; temporarily denying user access; and deploying inoculation software.

L.1 Standards

L.1.a) Each Agency must develop an Incident Response Plan (IRP), which identifies the responsibilities and actions to be taken in response to incidents.

L.1.b) The state's Security Center of Excellence is responsible for providing a communication vehicle(s) and establishing a service(s) in support of Agency incident handling.

L.1.c) Each Agency must ensure that out-of-band communication alternatives are established as part of their Incident Response Plan (i.e., that the "compromised" device, platform, or media is not used to notify users or to report the incident).

L.2 Best Practices

L.2.a) An Incident Reporting Plan (IRP) should detail the steps to be taken to identify, notify, contain, eradicate, recover from, record and report incidents. (E.g., a reference of a framework for an IRP is available from SANS Institute.)

M. Auditing System Activities

Auditing System Activities refers to those practices, technologies and/or services used to ensure that the implementation and maintenance of security safeguards and system changes are adequately documented and managed, such that accountability can be established.

Auditing System Activities provide a means to access policy compliance (e.g., security check list), verify operational assurance (e.g., penetration testing), maintain individual accountability (e.g., user audit trails, change management approvals), and to support intrusion problem analysis (e.g., user behavior anomalies; repeated failed log-in attempts; reconstruction of events).

Auditing System Activities can be self-administered (by the Agency) or independently administered (by parties external to the Agency). Personnel involved in these activities must have a high-level of expertise in the information technology security field and of auditing practices; and must administer said activities objectively.

Industry practices suggest that security safeguards tend to degrade over the operational lifecycle of systems as users and operators discover new ways to intentionally or unintentionally bypass or subvert security. Agencies must therefore make a risk-based decision regarding the timing (e.g., annual independent audit; daily audit log analysis) and scope (e.g., system, application or user level) of Auditing System Activities.

M.1 Standards

M.1.a) Each Agency must monitor and track systems, activities and operations, with resulting data made accessible, to ensure compliance and accountability with security policies.

M.1.b) Each Agency must include a configuration management process in their security program that establishes accountability for changes to information system components.

M.2 Best Practices

M.2.a) System configurations and software change over time. Therefore, each Agency should audit security devices, (e.g., firewalls, routers, secured servers such as E-mail gateways, etc.) on a periodic basis to determine if compliance to security policies is being met.

M.2.b) Each Agency should have a security audit performed by a qualified and approved auditing party external to that Agency on an annual basis as a supplement to internal auditing activities.

M.2.c) Each Agency should use a qualified and approved auditing party external to that Agency to perform E-Commerce audits on an annual basis.

Appendix A: "EA Common Requirements Vision" Implications

The "EA Common Requirements Vision" defines the following key elements that drive and/or influence the State's ability to design and deliver its core services:

- Technology Trends (TT),
- Enterprise Business Strategies (EBS), and
- Requirements for Technical Architecture (RTA).

These elements are detailed in the current version of the "Common Requirements Vision" (www.sotech.state.va.us/cots/ea/vision.htm). A cross reference of the implications of these elements on the Security Domain is shown in the tables below. The following "degrees of impact" are used by the tables:

- High Impact – Element has significant potential for influencing the security components in both the near-term and long-range.
- Medium Impact – Element exerts a strong influence on some aspect of the components within the architecture.
- Low Impact – Element does not drive decisions for the security components.

Table 1: Impact of Technology Trends (TT) on Security Architecture

High Impact	Medium Impact	Low Impact
TT01 – Widespread Access to the Internet by citizens.	TT07 – Technical workforce shortage.	TT09 – Enterprise server evolution.
TT02 – Internet and Intranets as dominant communications vehicles.	TT12 – Movement towards right-sourcing.	TT10 – Organizational dual discipline proficiency.
TT03 – Requirements for secure connections over the Internet.	TT15 – Increasing use of data warehouse technologies.	TT11 – Convergence of multimedia application and networks.
TT04 – Network centric computing.		TT17 – Customized service delivery.
TT05 – Electronic commerce expectations of business partners.		TT18 – Continued growth of OLTP.
TT06 – Emergence of Web browser as client of choice.		TT19 – Standardization of desktop workstations.
TT08 – Standardization on TCP/IP.		TT23 – Technology price performance curve continues to improve.
TT13 – Movement towards Enterprise Portals.		
TT14 – Increasing demand for mobile connectivity.		
TT16 – Rapid technology change.		
TT20 – Increase in Application hosting.		
TT21 – Increase in N-Tier computing.		
TT22 – Demand for enterprise systems management tools.		
TT24 – Improved availability of packaged solutions.		

Table 2: Impact of Enterprise Business Strategies (EBS) on Security Architecture

High Impact	Medium Impact	Low Impact
EBS01 – Focus on Customer Service.	EBS03 – Respond to needs of a growing , diverse population.	EBS02 –Improve quality of information and decision-making.
EBS05 – Balance freedom of information with privacy and security.	EBS06 – Identify and encourage improved service delivery mechanisms.	EBS04 – Attract, manage, and retain a highly skilled government workforce.
EBS08 – Promote continuous improvement.	EBS11 – Optimize service delivery through improved stewardship of limited resources.	EBS07 – Provide a technically educated workforce.
EBS09 – Improve procurement of goods and services.		EBS13 – Foster economic development.
EBS10 – Ensure IT Interoperability.		
EBS12 – Promote collaboration and cooperative systems development.		
EBS14 – Reduce gap between availability and adoption of technology.		

Table 3: Impact of Requirements for Technical Architecture (RTA) on Security Architecture

High Impact	Medium Impact	Low Impact
RTA01	RTA04	RTA02
RTA05	RTA06	RTA03
RTA07	RTA09	RTA08
RTA13	RTA19	RTA10
RTA14		RTA11
RTA15		RTA12
RTA16		RTA17
RTA23		RTA18
RTA24		RTA20
RTA25		RTA21
RTA27		RTA22
RTA29		RTA26
		RTA28

RTA Quick Reference

RTA01 EA must facilitate provision of information as a primary service of government in the information age.

RTA02 EA must enable deployment of appropriate service delivery directly to customers using cost effective technologies.

RTA03 EA must provide mechanisms to determine and adapt to the service delivery preferences of customers.

RTA04 EA must support implementation of multiple service delivery channels for the same service utilizing common underlying information and systems to enable rapid response to changes in business requirements.

RTA05 EA must provide the capability to locate and present information seamlessly based on the requestor's needs and context without requiring the requestor to know in advance the source or location of the information.

RTA06 EA must support delivery of latest relevant information.

RTA07 EA must enable provision of automated services consistent with customer needs and expectations in a cost effective and appropriate manner.

RTA08 EA must provide mechanisms to collect, continuously update, and use customer service and cost information. This includes: quantitative and qualitative information on customer needs; the quality, usefulness and access frequency of information or services; and the total cost of implementation and operation of service providing mechanisms.

RTA09 EA must support mechanisms to detect and resolve data discrepancies, incomplete data and incorrect data.

RTA10 EA must support collection and use of customer demographic data to allow customized delivery of services to a broad range of customer groups including those with special needs.

RTA11 EA must support collecting data on service delivery success linked to customer characteristics to facilitate provision of tailored services to different customer segments.

RTA12 EA must provide infrastructure that facilitates collection, analysis and sharing of recruitment data, retention data, and workforce availability information across all levels and branches of government.

RTA13 EA must protect the confidentiality and integrity of data being stored or transmitted.

RTA14 EA must support multiple levels of security, access control and audit capability.

RTA15 EA must facilitate ease of access to information within the constraints of privacy and security.

RTA16 EA must enable flexible sharing of service delivery channels to provide seamless customer service.

RTA17 EA must enable exchange of information about knowledge, skills and abilities (KSA) required for the workforce and about availability of KSA in the workforce between all levels of government and the business community.

RTA18 EA must facilitate delivery of education services to citizens of all ages across multiple delivery options including non-traditional times and locations wherever citizens need to learn.

RTA19 EA must provide a flexible and scaleable infrastructure to support rapid fluctuations in demand.

RTA20 EA must enable capacity, performance and configuration management, using real-time and historical metrics.

RTA21 EA must support rapid deployment and dependable operation of robust and flexible procurement systems to enable expeditious and efficient procurement of goods and services.

RTA22 EA must enable collection, analysis and sharing of procurement performance information to support a well managed and auditable procurement process.

RTA23 EA must support flexible implementation based on industry standards consistent with mainstream trends.

RTA24 EA must support multiple sets of standards to ensure interoperability.

RTA25 EA must facilitate collaborative development of applications and related technology projects by organizations whether or not physically co-located.

RTA26 EA must facilitate distributed project management.

RTA27 EA Architecture must enable deployment of common applications in both centralized and decentralized implementation as appropriate.

RTA28 EA must facilitate implementation of a high capacity and high availability technology infrastructure in all parts of the Commonwealth, in cooperation with business and industry that will attract businesses to the Commonwealth and promote widespread economic growth.

RTA29 EA must enable strategic prototyping of new technologies and rapid deployment of technologies and service delivery mechanisms determined to be effective, stable, and appropriate.

Appendix B: Related Websites and References

COVA Websites:

1. Commonwealth of Virginia Enterprise Architecture website:
   http://www.sotech.state.va.us/cots/ea

2. Council on Technology Services (COTS) website:
   http://www.sotech.state.va.us/cots

3. Link to Commonwealth of Virginia "ITRM Policies, Standards and Guidelines":
   http://www.dtp.state.va.us/policies_procedures.html

4. Contact for further information regarding Enterprise Architecture:

Paul E. Lubic, Jr., Manager
Virginia Department of Technology Planning
110 South 7th Street, Suite 135
Richmond , Virginia 23219-3931
(804) 371-0005, FAX (804) 371-2795)
plubic@dtp.state.va.us

Federal and Industry References:

1. *An Introduction to Computer Security: The NIST Handbook*, SP 800-12, National Institute of Standards and Technology (NIST), October 1995.

2. *Generally Accepted Principles and Practices for Securing Information Technology Systems*, SP 800-14, National Institute of Standards and Technology (NIST), September 1996.

3. Computer Security Special Publications Index, 800 and 500 Series, National Institute of Standards and Technology (NIST), February 2001.
   http://csrc.nist.gov/publications/nistpubs/index.html

4. *Security of Federal Automated Information Resources*, Appendix III to OMB Circular No. A-130, Office of Management and Budget (OMB), November 2000.
   http://www.whitehouse.gov/omb/circulars

5. Federal Information Processing Standards (FIPS) On-line
   http://csrc.nist.gov/publications/fips/index.html

6. Institute of Electrical and Electronic Engineers (IEEE) Standards On-line
   http://standards.ieee.org/catalog/olis/index.html

7. American National Standards Institute (ANSI) Banking and Security standards for Financial Services (X9F). www.ansi.org

8. "Common Criteria for Information Security Evaluation", ISO/IEC 15408
   http://csrc.nist.gov/cc/ccv20/ccv2list.htm

9. System Administration, Networking and Security Institute (SANS) [a cooperative education and research organization. www.sans.org

10. Internet Engineering Task Force (IETF). www.ietf.org

Appendix C: Glossary & Acronyms

Glossary:

Agency – The term "Agency" means executive branch Agencies and institutions of higher education.

Authentication – The term "authentication" refers to the process of verifying the identity of a user.

Authorization – The term "authorization" refers to the process of establishing and enforcing a user's rights and privileges to access specified resources.

Best Practice - The term "best practice" means a guideline or specification that is advisory in nature and whose compliance is strongly recommended; however, it is not binding on Agencies.

Critical (or Mission Critical) – The term "critical" refers to those information resources whose unavailability or improper use has the potential to adversely affect the ability of an Agency to accomplish its mission.

Data – The term "data" includes but is not limited to data in a database, information about an OS, operational policies and procedures, system design, organization policies and procedures, system status, and personnel schedules.

Emerging - One of four categories used in the domain report to guide technology use in the Commonwealth (see also obsolescent, strategic, and transitional). "Emerging" infers that the Virginia Enterprise Architecture promotes only evaluative deployments of this technology. This technology may be in development or may require evaluation in government and university settings.

Encryption – The term encryption refers to the process of converting computer data and messages to something incomprehensible by means of a key, so that it can be reconverted only by an authorized recipient holding the matching key.

Firewall Technology – The term "firewall technology" refers any combination of network hardware, network software, and host-based software used within an organization to prevent unauthorized access to system software or data in accordance with its security policy (e.g. includes routers with access list proxy gateways, host-based firewall software, and specialized password devices).

Information – The term "information" means any communication or representation of knowledge such as facts, data or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative or audiovisual forms.

Information Resources – The term "information resources" includes government information, information technology and associated personnel.

Information Systems - The term "information systems" means a discrete set of information resources organized for the collection, processing, maintenance, transmission and dissemination of information, in accordance with defined procedures.

Information Technology – The term "information technology" means any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information by an Agency. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services and related resources.

Obsolescent - One of four categories used in the domain report to guide technology use in the Commonwealth (see also emerging, strategic, and transitional). "Obsolescent" infers that the Virginia Enterprise Architecture actively promotes that agencies employ a different technology. Agencies should not plan new deployments of this technology. Agencies should develop a plan to replace this technology. This technology may be waning in use or no longer supported.

Open Standard – infers that the standard is not proprietary to a specific manufacturer, vendor, product or owner, but may be used among various components and products such that it facilitates interoperability; and it has been approved by an appropriate national or international standards body.

Out-of-band Communication – The term refers to a communication device, platform or media other than that communication media or platform on which a suspected or actual security threat is occurring. Thus, it becomes the alternative communication device, platform or media used to report an incident.

Owner - The term "owner" refers to that group (i.e., Agency or Agency unit) which controls a set of information resources and determines its level of criticality and sensitivity. As such, they determine access, authorization rights, and dissemination regarding those resources.

Public network – refers to that network infrastructure not controlled by the Agency (e.g., Internet, COVANET).

Policy – The term policy means any general statement of direction and purpose designed to promote the coordinated planning, practical acquisition, effective development, and efficient use of information technology resources.

Sensitive Information – Sensitive information refers to any confidential or critical information for which the loss, misuse, or unauthorized access to or modification or improper disclosure could adversely affect the Commonwealth's interest, the conduct of Agency programs, or the privacy to which individuals are entitled.

Standard - The term "standard" means a directive or specification whose compliance is mandatory, and whose implementation is deemed achievable, measurable, and auditable for compliance**.**

Strategic - One of four categories used in the domain report to guide technology use in the Commonwealth (see also emerging, obsolescent, and transitional). "Strategic" infers that The Virginia Enterprise Architecture promotes use of this technology by agencies. New deployments of this technology are recommended**.**

Transitional - One of four categories used in the domain report to guide technology use in the Commonwealth (see also emerging, obsolescent, and strategic). "Transitional" infers that the Virginia Enterprise Architecture promotes other standard technologies. Agencies may be using this technology as a transitional strategy in movement to a strategic technology. This technology may be waning in use or no longer supported.

User – An individual or group who has access to an information system or its data.

Acronyms:

APR – Agency Procurement Request

CIRT – Computer Incident Response Team.

CISA – Certified Information Systems Auditor.

CISSP – Certified Information Systems Security Professionals.

COVANET – Commonwealth of Virginia Network; the Commonwealth's statewide telecommunications network administered by the Department of Information Technology which includes wide-area network, long distance services, and other related services.

COVITS – Commonwealth of Virginia Information Technology Symposium.

EBS – Enterprise Business Strategy.

FTP – File Transfer Protocol.

HIPAA – Health Insurance Portability and Accountability Act.

HVAC – Heating, Ventilation and Air Conditioning.

IETF – Internet Engineering Task Force

IPSec – Internet Protocol Security.

IRP – Incident Reporting Plan.

ISSO – Information Systems Security officer (agency-level).

OS – Operating System.

NIST – National Institute of Technology.

PGP – Pretty Good Privacy (a security product name).

PKI – Public Key Infrastructure.

RTA – Requirement for Technical Architecture.

SANS – Systems Administration, Networking and Security (a cooperative research organization).

SHTTP – Secure Hypertext Transfer Protocol.

SSH – Secure Shell Protocol.

SSL – Secure Socket Layer.

TCP/IP – Transmission Control Protocol/Internet Protocol.

TT – Technology Trend.

VPN – Virtual Private Network

Appendix D: Summary List of Standards by Component

A.1 Business Analysis and Risk Assessment

A.1.a) The head of each Agency shall be responsible for the security of the Agency's information resources; and formally appoints an Information Systems Security Officer (ISSO) who is responsible for the development, implementation, oversight, and maintenance of the Agency's information security program.

A.1.b) Each Agency must establish, document, implement and maintain an information security policy and program appropriate to its business and technology environment. The policy and program must be consistent with Federal regulations (e.g., H.I.P.A.A; Rehabilitation Act Sec. 508) and State laws (e.g., Virginia Privacy Protection Act of 1976).

A.1.c) Security program documentation must specify how exceptions to security standards are to be handled. All such exceptions must be completely reviewed by a level of management above that approving the exception.

A.1.d) Each Agency must conduct a business impact analysis and risk assessment throughout the Agency (to include relevant business partners) to identify various levels of sensitivity associated with the information resources as defined; to identify the potential security threats to those resources; and to determine the appropriate level of security to be implemented to safeguard those resources. The business impact analysis and risk assessment can be reviewed and updated as needed, but at minimum must be reviewed and updated every three years.

A.1.e) Security programs must include protective measures and procedures to ensure that the appropriate levels of confidentiality, integrity and availability of data, information, and systems are sustainable.

A.1.f) Development, installation and/or changes to the Agency environment, technical infrastructure, and information systems must be reviewed for security implications and approved by the Agency's ISSO, or by person(s) delegated said approval authority by the Agency's ISSO, as part of the planning and design process; and then coordinated thoroughly during development and implementation. Acknowledgement of this review and approval by the Agency's ISSO, or delegated authority, must be documented and auditable.

A.1.g) Security programs must be coordinated and integrated with contingency planning and business resumption activities.

B.1 Security Awareness

B.1.a) Each Agency must establish and maintain information technology security awareness programs to ensure that all individuals are aware of their security responsibilities and know how to fulfill them.

B.1.b) A security awareness training program must:

- be approved by the Agency's Information Systems Security Officer (ISSO);
- specify timeframes for receiving training (initial, ongoing and/or refresher);
- provide both general and position appropriate security awareness content; and
- be documented on an auditable medium.

B.1.c) All new hires must attend formal security awareness training as designed by their Agency within 30 calendar days of their start date.

B.1.d) Receipt of Security Awareness Training must be documented in the employee's personnel file with employee's acknowledgement of receipt and understanding.

B.1.e) Security Awareness Refresher Training must be provided to personnel annually at a minimum.

C.1 Technical Training

C.1.a) Each Agency must establish and maintain information technology security training programs to ensure that all individuals involved in managing, administering, designing, developing, implementing, and/or maintaining information resources are aware of their security responsibilities and know how to fulfill them.

C.1.b) Information technology security training programs must be commensurate to the level of expertise required for the system components and information resources for which they are responsible. The program must include content that enables the individual to identify and evaluate threats, vulnerabilities, and risks specific to those components and resources. The program must further include content regarding technical alternatives, methods, and standards which represent best practices appropriate to those components and resources, and which can be utilized to effectively implement safeguards as appropriate.

D.1 Technical Communications

D.1.a) Each Agency must subscribe to the technical security dissemination service(s) provided by the state's Security Center of Excellence. Each Agency must disseminate information received through the above service(s) to the appropriate personnel within their organization in a timely manner.

D.1.b) If any data or documentation contains sensitive information, then the Agency must ensure that such information is given accountable and authorized dissemination only.

E.1 Authentication, Authorization and Encryption

E.1.a) Each Agency must ensure that Users are authenticated prior to accessing the systems which are "owned" by that Agency.

E.1.b) Each Agency must establish a formal authentication control policy that establishes the criteria for administering authentication safeguards.(e.g., a formal password policy that includes the criteria for password aging, history, length and composition).

E.1.c) Each Agency must store all sensitive data used in authenticating the user, including passwords, in protected files.

E.1.d) Public key certificates must be based on the most current IETF X509 standards.

E.1.e) Each Agency must authorize based on least privilege. Least privilege states that a user is given only that set of privileges necessary to perform his/her job.

E.1.f) The use of cryptology technologies for data storage and data communications (transmission of data) must be based on open standards.

E.1.g) All Virginia On-Line Transaction (VOLT) Certificates utilized by an Agency must be issued by service providers who are currently granted "Authorized Certificate Authority" status via a Virginia VOLT contract.

F.1 Data Security

F.1.a) Ownership of data must be specifically identified by each Agency. [Note, based on the Agency's business impact analysis and risk assessment referred to Section A, files and data elements to be protected will be identified.]

F.1.b) Owners are responsible for determining the appropriate levels of data security required.

F.1.c) All sensitive data must be removed from system hardware, software or media by the owner prior to its "reuse" by another Agency, or for "reuse" by another system within the Agency. Similarly, all sensitive data must be removed from system hardware, software or media by the owner prior to its disposal.

G.1 Systems Interoperability Security

G.1.a) Each Agency must ensure that authentication, authorization and data security, as established by the data owner, is not compromised during data sharing and systems interoperability.

G.1.b) Auditable user agreements must be established between the Agencies sharing data, which clearly state the degree of authentication and levels of protection required.

G.1.c) Web-enabled transactions that require user authentication, or transfer of sensitive data, or that involve the transfer of funds, must use encryption (e.g. SSLv3).

H.1 Physical Security

H.1.a) Mission critical system facilities must be located in a secure location that is locked and restricted to authorized personnel only.

H.1.b) Access to "critical" computer hardware, wiring, displays and networks must be controlled by rules of least privilege.

H.1.c) System configurations (i.e., hardware, wiring, displays, networks) of "critical" systems must be documented. Installations and changes to those physical configurations must be governed by a formal change management process.

H.1.d) A system of monitoring and auditing physical access to "critical" computer hardware, wiring, displays and networks must be implemented (e.g. badges, cameras, access logs).

H.1.e) Back-ups of mission critical data must be stored off-site in a secured location.

I.1 Personnel Security

I.1.a) Access must be explicitly granted to personnel by the Owner (i.e., not allowed by default).

I.1.b) Access granted to personnel must be based on least privilege (i.e., only up to the level needed to perform one's duties).

I.1.c) Access must be terminated concurrent with when the requirement for access no longer exists (e.g., as result of transfer, termination , and change of duties).

J.1 Threat Detection

J.1.a) Each Agency must establish and implement a process to identify and evaluate threats and assign appropriate action based on risks.

J.1.b) Firewall technology must have security logging turned on**.**

K.1 Security Tool Kit

K.1.a) Agencies with external connections using TCP/IP must utilize firewall technology.

K.1.b) Each Agency must test its firewall technology on a periodic basis to ensure compliance with security policies.

K.1.c) Each Agency must deploy multi-layered protection at the internet gateway, the network server and the desktop levels to prevent the introduction of malicious code into the system.

L.1 Incident Handling

L.1.a) Each Agency must develop an Incident Response Plan (IRP), which identifies the responsibilities and actions to be taken in response to incidents.

L.1.b) The state's Security Center of Excellence is responsible for providing a communication vehicle(s) and establishing a service(s) in support of Agency incident handling.

L.1.c) Each Agency must ensure that out-of-band communication alternatives are established as part of IRP (i.e., that the "compromised" device, platform, or media is not used to notify users or to report the incident).

M.1 Auditing System Activities

M.1.a) Each Agency must monitor and track systems, activities and operations, with resulting data made accessible, to ensure compliance and accountability with security policies.

M.1.b) Each Agency must include a configuration management process in their security program that establishes accountability for changes to information system components.

Appendix E: Summary List of Best Practices by Component

A.2 Business Analysis and Risk Assessment

A.2.a) In assigning the level of risk, each Agency should evaluate both the probability of an event occurring and the resultant effect of that event on the confidentially, availability, and integrity of system components and data.

B.2 Security Awareness

B.2.a) Security Awareness programs should contain content that covers, but is not limited to:

- Responsibility of users to report issues;
- Users can be audited;
- Legal requirements for data (citing legislation as appropriate);
- Privacy expectations;
- Ownership of data;
- Acceptable use policy for E-mail and Internet Browsers; and
- Sensitivity to threats, risks, vulnerabilities.

B.2.b) Security Awareness programs should include a means to promote security awareness on an on-going basis, i.e., supplemental to training (e.g., security awareness banners, posters, "security day", etc.)

B.2.c) Security Awareness training content is not static, and should be continuously reviewed and updated by each Agency as needed to reflect changes to the Agency's environment, business, technology, systems and information.

C.2 Technical Training

C.2.a) Each Agency should consider using certification programs to promote high-level, up-to-date technical security expertise (e.g., CISA, CISSP or SANS).

D.2 Technical Communications

D.2.a) Each Agency should subscribe to industry and vendor security mailing lists for the appropriate system components used within, or interfaced by, the Agency.

D.2.b) Organizations should consider and encourage including information security topics in conferences, symposia, seminars, etc., where appropriate (e.g., the Commonwealth of Virginia Information Technology Symposium (COVITS)).

E.2 Authentication, Authorization and Encryption

E.2.a) Each Agency should identify a method of verifying user authenticity on a spectrum from "null/weak" to "strong" authentication methods. Authentication is based on validating the following three criteria presented by the user: 1) "What do you know?", 2) "What do you have?", and 3) "Who are you?". Weak authentication is based on validating one of these criteria only, and should only be used when a minimum level of authentication is desired. Strong authentication, which is based on validating two or more of the criteria, should be used in all other cases.

E.2.b) Each Agency should establish policy and procedures that address when different levels of encryption, digital signatures, and digital certificates are appropriately used.

E.2.c) Digital signature and digital certificate technology can be used by Agencies to verify the authenticity of electronically transmitted data. If high-assurance digital certificates are deemed appropriate, Agencies should use either Virginia On-Line Transaction (VOLT) Certificates, or high-assurance certificates that are compatible with VOLT Certificates.

E.2.d) With regards to Digital Signatures, Agencies should use the VOLT Public Key Infrastructure wherever possible, and should adhere to the Internal Control and Auditing practices established to support the use of digital certificates in the Commonwealth.

E.2.e) Each Agency should establish Encryption Key Management policy and procedures to address the integrity and recovery of the "keys".

E.2.f) Each Agency should identify criteria governing the number of unsuccessful login attempts allowed by a user, and the resetting of passwords.

E.2.g) Authorization should use role-based access models.

E.2.h) Each Agency should use single sign-on technology where appropriate**.**

E.2.i) Each Agency should strongly consider encryption to protect sensitive data, including passwords, that are transmitted over a public network (e.g., replace Telnet with SSH).

E.2.j) Each Agency should strongly consider encryption to protect sensitive data, including passwords, transmitted over an internal network.

F.2 Data Security

F.2.a) Desktop platforms, including laptops, should have a protected screen saver mechanism, which is activated.

F.2.b) Automatic protected screen savers should be initiated by the system after a specific period of inactivity.

F.2.c) Auditable user agreements should be utilized to delegate responsibility for data security from data owners to data custodians. Custodians are responsible for ensuring that the levels of required protection are followed.

G.2 Systems Interoperability Security

G.2.a) Agencies should use open standard-based security solutions, as opposed to unique generated security solutions, to support current interoperability needs and to position them for future interoperability needs.

G.2.b) Agencies should use open standard based encryption algorithms when sharing sensitive data internally; and externally for data that requires encryption that is resident on that system.

G.2.c) New deployments of VPN (Virtual Private Network) technologies should use IPSec (Internet Protocol Security).

G.2.d) E-mail should not be considered a secure transport in itself. Therefore, any attachment containing sensitive information should be encrypted (e.g., using Pretty Good Privacy (PGP)).

G.2.e) Unencrypted Telnet, FTP, or R-Utilities should not be used.

G.2.f) Secure Shell Protocol (SSH) and Secure Hypertext Transfer Protocol (SHTTP) should be deployed for remote terminal sessions and file transfers.

G.2.g) 40 bit encryption should be used with SSL transactions to ensure global interoperability unless there is a requirement to use a higher bit encryption. (E.g. Virginia Militia or Virginia citizens residing overseas may be limited to 40 bit encryption.)

G.2.h) 1024 bit key digital server certificates should be used for SSL.

G.2.i) Agencies using digital certificates should seek interoperability with those digital certificates utilized by other government bodies(Federal, State, and Local). Virginia On-Line Transaction (VOLT) Certificates are designed for such compatibility.

H.2 Physical Security

H.2.a) Mission critical system components should be located in an environmentally friendly area (e.g., which includes fire protection, HVAC, UPS).

H.2.b) Access to computer hardware, wiring, displays and network should be controlled by rules of least privilege.

H.2.c) System configurations (i.e., hardware, wiring, displays, network) should be documented. Installations and changes to those physical configurations should be governed by a formal change management process.

H.2.d) Physical Access security for back-up systems should be equivalent to that of the primary facilities.

H.2.e) A system of monitoring and auditing physical access to computer hardware, wiring, displays and networks should be implemented (e.g., badges, cameras, access logs).

I.2 Personnel Security

I.2.a) Each Agency should establish and document the process which directs the steps and the timing required to grant and withdraw physical and system access privileges to personnel for the following events: new hire, employee transfer to another Agency, employee termination, employee resignation, employee change of job duties within an Agency, and perceived disgruntled employee behavior. A similar process should be established for contractors (i.e., non-state personnel) working for or on behalf of an Agency.

I.2.b) System access should be granted via a formal and auditable process, and should be accompanied by security training which is commensurate to one's duties and responsibilities.

I.2.c) Non-Disclosure Agreements should be signed by all individuals who need access to "sensitive" information, prior to granting access to that information.

I.2.d) Background checks of personnel may be required consistent with Agency policy and depending on the sensitivity of information accessible to that position.

J.2 Threat Detection

J.2.a) Violations of those parameters set in conjunction with the Agency's threat detection program should trigger an appropriate form of security notification to security administrators or security staff.

J.2.b) Systems should be designed to handle both passive and active alarms.

J.2.c) A security event log should be kept for each device. These logs should be analyzed, correlated and evaluated to identify and respond to suspicious activity.

J.2.d) Security logs should be archived on a daily basis.

J.2.e) Security logs should be moved off the device as soon as possible and stored on an off-site location.

J.2.f) Intrusion detection systems should be deployed both externally and internally to the firewall technology protecting the network.

J.2.g) Agencies should get assistance from the Computer Incident Response Team (CIRT) provided by the state's Security Center of Excellence as needed to trouble shoot unusual or "difficult to isolate" threats.

K.2 Security Tool Kit

K.2.a) Within the Agency, firewall technology should be implemented to protect sensitive internal information.

K.2.b) Each Agency should have the ability to monitor and capture traffic at any location within their network (e.g. via use of a portable sniffer).

K.2.c) Each Agency should use network and host vulnerability scanners to test for the vulnerabilities of internal systems and of perimeter defenses, and their adherence to security policy. Resulting vulnerabilities should be addressed.

K.2.d) Each Agency should scan all incoming e-mail for existence of malicious code (e.g., viruses), and contain and eradicate that code.

K.2.e) Each Agency should keep Virus signatures current by updating virus signatures weekly at a minimum.

L.2 Incident Handling

L.2.a) An Incident Reporting Plan (IRP) should detail the steps to be taken to identify, notify, contain, eradicate, recover from, record and report incidents. (E.g., a reference of a framework for an IRP is available from SANS Institute.)

M.2 Auditing Systems Activities

M.2.a) System configurations and software change over time. Therefore, each Agency should audit security devices, (e.g., firewalls, routers, secured servers such as E-mail gateways, etc.) on a periodic basis to determine if compliance to security policies is being met.

M.2.b) Each Agency should have a security audit performed by a qualified and approved auditing party external to the Agency on an annual basis as a supplement to internal auditing activities.

M.2.c) Each Agency should use a qualified and approved auditing party external to that Agency to perform E-Commerce audits on an annual basis.