U. S. Railroad Retirement Board

Security/Privacy Domain Architecture

Security/Privacy Domain Architecture
Table of Contents

Security/Privacy Domain Definition

The purpose of the Security Architecture Domain is to protect the availability, confidentiality, and integrity of all information resources created, received, provided and maintained by the RRB. Information resources includes:

- data and information
- physical security,
- hardware/software,
- contingency planning,
- services, and
- personnel security,

Security Architecture identifies criteria, technology and techniques associated with the above. It will provide standards for identification, authentication, administration, authorization, disposition, audit and naming conventions.

Security/Privacy Domain Technology Categories

- Access Control and Authentication
- Anti-Virus Products
- Awareness Tools
- Biometrics
- Firewalls
- Encryption
- Intrusion Detection
- Security Administration
- Software Controls
- Physical Security
- Telecommunication and Remote Access Security

Security/Privacy Domain Principles Summary

1. Centralize Security Policy, Training and Oversight Functions
2. Centralize Security Administrative Maintenance Operations
3. Security will be Commensurate with the Business Need/Mandate
4. Minimize the Number of Security Devices
5. Consider Security During Initial System Design
6. Security should Ensure but NOT Impede Connectivity
7. Assign Security Levels Consistently
8. Provide Security to enable E-businesses
9. Provide Security Awareness Education and Technical Training

Domain Relevant Trends

- There is a general increase in the public's desire for privacy and confidentiality protection for reasons such as preventing identify theft.
- Presidential Directive Document PDD-63 requires vulnerability studies of critical systems to ensure that information resources are protected.
- There will be an increasing demand by the Board's customers for access to data.
- The need to house data off site will become increasingly necessary as the RRB uses contractors to perform certain functions. The off site storage of data introduces new vulnerabilities that need to be addressed.
- The e-government mandates will result in more types of interactive transactions and data exchanges that will require nonrepudiation security.
- The policy trend is to withhold less information from the public and to promote greater openness to public scrutiny.
- Public Key Infrastructure (PKI) will become an increasingly common and effective security measure to use for authentication and identification.
- GISRA requires that government agencies utilize intrusion detection software.
- Wireless and handheld devices are becoming more common and may be used to support some Board services, such as field service itinerant service.
- The need for network perimeter protection, such as home firewalls, will increase as the RRB's Work at Home program becomes widely used.
- There will be an increase in data sharing with other Federal and state government agencies.
- There will be increasing pressure from the public to match the WEB/Internet services available on other Web sites.
- The Government Paperwork Elimination Act (GPEA) mandates an increase in paperless processing.
- There will be an increasing need for security and computer awareness training for employees, customers and partners.
- Single sign-on and digital certificates technologies will become more widely used.
- Smart card technology will improve and become more prevalent. This technology can be used to support telecommuting.
- Audit/tracking software tools will be used increasingly to monitor security.
- The use of pin and password technology will be used for internal and external business transactions.

Background of Security/Privacy and Related Technologies at the RRB

The RRB is faced with the challenge of satisfying growing customer expectations of choice and quality in service delivery. The agency's strategic plan envisions the cost-effective use of technology to meet or exceed these customer expectations. The agency also looks to technology to leverage its workforce in an environment of increasing service options and decreasing budgetary resources. The best way to achieve success under these constraints is to use electronic media to maximize the availability and variety of services. Congress has recognized this by passing legislation requiring Federal agencies to make their services available in electronic formats.

The RRB's efforts to expand customer services and the capabilities of its workforce are changing the agency's traditional ways of doing business. The RRB's current services, or future plans, encompass service over a virtual private network, the Internet, an extranet, and through an interactive voice response system. The RRB is increasing use of mobile computing to support outreach service and is implementing a work-at-home program. The RRB will increasingly need to interconnect with other Federal agencies to make these services efficient and reach their full potential. And the RRB will employ vendors, such as a website host, to carry out parts of its service delivery.

At the same time that the RRB is expanding electronic business processes to meet public demand for access and to achieve higher efficiency, the public is demanding that its records be protected from improper use and disclosure. Identity theft has become a national issue, raising public concerns and awareness of the need for privacy. Congress has responded with additional statutes that require Federal agencies to protect the privacy of records. And agencies with which the RRB does business are requiring specific security measures if the RRB is to use their data.

These new ways of doing business and the need to protect privacy are leading the RRB into new security technologies. The RRB must employ firewalls to protect information resources that accessible through the Internet from unauthorized access, alteration and use. Electronic applications and claims for benefits require authentication technologies such as a public key infrastructure. E-mail with personal information must be encrypted, and the wireless technology that expands our range of service outreach must be secure.

The impacts of proliferating electronic processes and legislative mandates require that the RRB establish a well-coordinated approach to security for information resources. The alignment of security responsibilities, and the security infrastructure, must fully protect our information resources while enabling and not impeding high-quality service to our customers. All this must be achieved in a cost-effective manner.

The security domain architecture addresses these challenges. Its principles ensure effective coordination of security policy and administration and guide design and procurement decisions to ensure that products provide security and integrate well. It also serves as a resource for staff considering new security technologies.

Computer security plans - In accordance with the Computer Security Act and OMB Circular A-130, *Management of Federal Information Resources*, the Railroad Retirement Board has identified and prepared computer security plans for seven Major Application Systems and two General ADP Support Systems. An Administrative Circular provides guidance for preparing computer security plans for these systems.

The following pamphlets have been prepared and distributed to provide various types of security/privacy awareness and training:

a) *Information Systems Security Awareness Training for the Railroad Retirement Board* provides basic security training. The pamphlet is provided to all new employees, who are required to sign an acknowledgment statement that they have read and understand their security responsibilities.
b) *Security Training for Users of SSA Databases* provides training to employees who have online access to SSA databases on safeguarding the information.
c) *Information, Privacy, and You* provides training to employees on rights and responsibilities under the Privacy and Freedom of Information Acts.
d) *Business Information and You* provides employee training on responsibilities regarding their use of business information.

During fiscal year 2000, the RRB received an assessment of its information security by the National Security Agency (NSA). This assessment resulted in a comprehensive report including several recommendations concerning security improvements. Several improvements are underway including the implementation of a formal password management policy, enhanced virus protection, and establishing a formal computer security program.

Contingency Planning - The agency-wide contingency plan includes critical mainframe, personal computer, and manual applications. The plan identifies 335 applications, separated into four contingency categories based on priority requirements. It is available on compact disk (CD) and the Intranet (RRBnet) to provide for wider distribution of the information. The RRB has a contract through GSA for using Comdisco Disaster Recovery Services and mainframe and personal computer and local area network (LAN) recovery operations are tested twice a year at our recovery site.

Personal Computer/Local Area Network - During 1999 we relocated all file servers to the data center Virtual-Local Area Network (V-LAN) room to provide temperature and humidity control for the equipment and better physical security. Access to the V-LAN room is with an electronic key card.

The RRB has one Cisco PIX firewall running the proprietary IOX operating system version 4.2.3. The firewall provides full or intermediate access to the Internet. However, all public addresses are denied access to the firewall. All services inbound and outbound are denied except HyperText Transfer Protocol (HTTP). The initial configuration of the firewall was based on the needs of the agency. No authentication exists at the firewall and no auditing occurs on firewall accesses.

Plans are in progress to consolidate the back-ups of the individual file servers from the mainframe computer and transfer the data to an off-site facility on a weekly basis .We also plan to establish a Virtual Private Network (VPN) as a secure method of moving private data between end points across a public network, i.e. Internet.

The ADP Steering Committee approved the Norton anti-virus software as the agency standard. The anti-virus software is pre-loaded on new PCs and we have installed a dedicated server that automatically updates signature virus data to users PCs at both headquarters and the field service.

Mainframe Computer - Our mainframe computer is an IBM 390 processor, model 2003-2C5 with Complimentary Metal-Oxide Semiconductor (CMOS) technology. An internal battery feature will save the RRB the cost of purchasing a separate uninterrupted power source and will allow for the orderly shutdown of the operating system in the case of a power outage.

We replaced our tape library with a Virtual Tape Server. The technology automates and improves tape handling and almost never requires an operator to respond to routine tape-mount requests. The features should virtually eliminate program delays and abends resulting from lost or misfiled tapes and delayed mounts.

We recently upgraded the access control facility software package, CA-ACF2, to release 6.3 to meet additional security concerns. A more reliable method of backing up agency data stored on LANs will be implemented later this year through the use of ADSTAR Distributed Storage Manager (ADSM) and ADSM Disaster Recovery Manager software on the mainframe.

Application Development - We also replaced a mainframe-based software change control system, which was not Y2K compliant, with the Computer Associates' product, Endevor. The new system provides a better control environment for applications that we have developed in-house and for the commercial off-the-shelf applications that we use for our administrative/financial and human resources systems.

Domain Principle 1

Centralize security policy, training, and oversight functions

Centralize the development of security policies and procedures, technical training, security awareness education and oversight of the security/privacy responsibilities.

Rationale:

Promotes higher quality resolution of security related problems
Provides better accountability
Facilitates greater security comprehensiveness across RRB
Promotes consistent policy and practices.
Meets legislative and regulatory mandates.
Provides better coordination for the functions

Implications:

Requires the development of an audit policy, procedures and program.
Policy and procedures must accommodate special handling of justified exceptions such as SSA, and IRS data.
RRB security policy must cover directives for incident response and the logging of security events.
The roles and responsibilities for carrying out various aspects of policy and procedures must be defined.
Requires the creation/appointment/identification of an RRB security official
Need to develop/acquire/identify appropriate awareness and training for all users of RRB information technology.
Security policy must address physical security (PDD-63).
Maintains Sensitive Systems Assessment (CSA).
Comply with OMB Circular A-130
Requires the development of security Standards Profile.
Coordinates vulnerability Assessments (PDD 63)
GIRSA requires:

- that program officials must review each agency-wide information security program annually;
- Examine the adequacy and effectiveness of information security policies, procedures, practices and report weaknesses;
- Integrate security in Capitol Planning; and
- Develop security plan performance measures.

Domain Principle 2

Centralize security administrative maintenance operations
Operational security functions for all platforms will be centralized at the most appropriate level. The operational security functions includes: password maintenance, access controls, day-to-day monitoring of networks, firewalls, routers, communication lines, and incident response.

Rationale:

Provides for a higher-quality resolution of security related problems.
Reduces the complexity of the IT environment.
Simpler to maintain/lower cost.
Fosters/allows for separation of duties.
Provides better accountability.
Minimizes duplication.
Will lessen the burden on Help Desk
Supports integration of security services
Will facilitate "one stop" access granting

Implications:

Will reduce the number of security administrators
Complicates the administration of applications
Monitoring intrusion detection devices should be included.
Focuses on reducing access problems for the user/partners/customer.
Need to develop access controls on our PC's platforms similar to those used on the mainframe.
May require the purchase of additional products, services and training.
Will still require coordination among uncentralized applications.

Domain Principle 3

Security commensurate with need/mandate
Security will be commensurate with the business needs and legislative mandates.

Rationale:

Will avoid unnecessary costs by NOT providing more security than needed. Security costs should be rationalized to the intended benefit.
Keeps the RRB in compliance with applicable laws.
Allows the mission needs to drive security investments.
Will not block important business needs but still ensures that security is sufficient.
Supports a risk-based security program.

Implications:

The system design process will assess system/application risk or vulnerability versus value achieved from security and include development plans/approaches to mitigate risk. (GISRA).
The user and IT components must understand the priority of the business requirements of the process and the sensitivity of the data involved.
"One size" security approach will not be appropriate for all business processes/situations.
The users who determine systems design will need to identify and understand (and keep current with) legislative and regulatory requirements.
Security considerations are not the driving consideration (except in certain special situations) when developing applications.
Requires an effort to understand the need of the RRB's internal and external partners.
RRB's security policy must be expanded to include work at home.

Domain Principle 4

Minimize the number of security devices

Use the minimal number of security devices appropriate to consistently achieve the security needed for the specific system/application. Re-use/leverage existing security devices, where possible.

Rationale:

Fewer devices reduces complexity.
Makes security simpler and easier to maintain.
Fewer devices will lower the burden on the Help Desk.
Minimizes redundancy.
Allows for more efficient and secure administration of security, lowering staff cost.
Simpler mechanisms tend to have fewer exploitable flaws and require less maintenance.
Eases integration of security services
Easier to change and upgrade security devices

Implications:

RRB will need to leverage/reuse existing security services.
RRB must simplify security administration (procedures).
Security administration must use industry or existing RRB standards where possible.
Greater use of client/server and the internet/web may require the adoption of a security server or tier in the architecture.
Need to develop a catalogue of current devices that can be reused.
We may need to choose between security built into platforms verses the need for stand-alone security devices
We must consider scalability of security devices as well as the number of devices.

Domain Principle 5

Consider security during initial system design

Security requirements will be identified as part of the project definition phase and addressed during subsequent systems development (SDLC) (mainframe/PC) phases.

Rationale:

Facilitates the integration of security functionality.
Enhances shorter development cycle times
Adheres to RRB System Development Lifecycle (SDLC).
Decreases retrofitting; it is difficult to implement security measures properly and successfully after a system has been developed.
Increases the effectiveness of the security measures in place
GISRA mandates a risk-based security program throughout the SDLC.

Implications:

During the design, we will need to develop an understanding of security risks associated with the proposed application/system and method of deployment.
System requirements must consider data security needs of application transmissions and storage.
During design, we must identify security requirements from our internal and external business partners.
Requires that we ensure that the proper security measures are in place when conducting business with external vendors and contractors.
Integrating security into systems design includes the security requirements, participating in the evaluation of security products, and finally in the engineering, design, implementation and disposal of the system.

Domain Principle 6

Security should ensure but not impede connectivity

Security features need to be sufficient to prevent the interruption of connectivity due to hostile activities and/or threats while NOT impeding authorized users' connectivity.

Rationale:

Will foster greater systems or network availability.
Enhances productivity.
Will result in cost saving through greater system availability.
Increases compliance with security measures.
Improves customer service.

Implications:

May require redundancy in certain RRB IT assets.
Security configurations must be designed to have minimal impact on performance.
The RRB should investigate intrusion security devices.
Increases testing requirements to implement new security devices.
Security administrators must keep current with new software updates (e.g., anti-virus, patches).

Domain Principle 7

Assign security access levels consistently

Security access must be granted based on standard factors such as the:

- *type of data,*
- *type of the user,*
- *intended use of the application, and*
- *location of the user.*

Rationale:

Provides for greater ability to grant access on the "need to know" basis.
Fosters consistency of security application
Establishes model(s) for future access needs
Provides for easier security administration
Makes it easier to define security requirements for new applications

Implications:

Data and application profiles should be established and maintained for users. Profiles should consider the level of identification, authentication and non-repudiation required for the application, based on who the user is and what functions they will perform with the application.
Profiles will need to be developed in accordance with applicable security policies.
A security matrix/profile will need to be developed for service requests.
A "profile" concept needs to be incorporated into contracts with external vendors/partners
Need to develop and deliver awareness, education and training to users and systems administrators.
User identification required for data access.
System design needs to consider how the data is stored, transmitted, presented and exchanged.
Revision of the principle may be required as we gain more experience in this area.
Will need to determine the appropriate access levels.

Domain Principle 8

Provide security to enable e-business

Provide infrastructure security services to enable the RRB to conduct business electronically.

Rationale:

Supports requirements of the Government Paperwork Elimination Act and E-government mandates.
Supports the agency goal of "One and Done".
Addresses customer service needs.
Allows the RRB to conduct business over the Internet, Intranet and Extranet.
Supports RRB strategic goals.
Permits the RRB to focus on business goals.

Implications:

Development procedures needed to identify/develop an approach for change control.
Need to develop corresponding policies and procedures, standards and practices.
Some applications will require two-way authentication.
Requirements must apply the appropriate security devices necessary to allow safe/secure connections for our external partners.
The RRB must aggressively utilize encryption devices.
More e-business increases vulnerability.
Principle3 must be taken into account when security for RRB e-business is being considered.

Domain Principle 9

Provide security awareness, education and technical training

Provide security awareness, education and training for all users and security administrators.

Rationale:

Enhances user buy-in and understanding, thus increasing the degree of compliance.
Increases the awareness of security standards and policies (CSA).
Provides for more effective security administrators and developers.
Enhances employee productivity (e.g., educated users can prevent problems from occurring thus avoiding downtime associated with an occurrence. Users will know who to call when they have a problem,)

Implications:

Training plans should balance formal versus informal training.
Different training will be required based on roles and responsibilities.
Training plans should consider the security guidance provided by NIST.
Need to develop policy and procedures upon which to base the training.
Requires the RRB to develop/acquire/identify appropriate training and education.
Requires the RRB to develop or update relevant IT Standards.
The experience and expertise of administrators and users should be appropriate and proportional to the operation of the security measure. The RRB must invest resources to ensure that system administrators and users are properly trained.
Procurement decisions must consider security-training needs.
Users need to be aware that IRS and Privacy Act data along with data mentioned in the RRB pamphlet, *Business Information and You*, is prohibited from being included in an electronic message (email).
Requires change control procedures of profiles, software etc. be established and followed.

Pattern 1

Establish patterns/profiles required for access to specific data types.

Purpose

Establish a pattern/configuration for the following types of data: IRS, SSA, RRA/RUIA, Data subject to the Privacy Acts, Business Information and others.

Applicability

TBD

Assumptions

TBD

Structure Overview

Data Security Profile	
IRS Data	
SSA Data	
Risk Based	RRA/RUIA Data
	Data subject to the Privacy Act
	Business Information
	Other

Detailed Pattern Description

TBD

Benefits

TBD

Consequences

TBD

Variations

TBD

Related Patterns

TBD

Known Uses

TBD

Domain Participants

Domain Team Leader: Claudia Jackson (Alternate: Robert Piech)

Line of Business Representatives: Rita Jackson, Douglas Fager, Leroy Blommaert

Domain Participants: Philip D'Agostino, Rosalie Klocek, Phil Arnold, Pauline Coleman-Sutton, Vaidevutis Zemaitis, Leon Tetzlaff

APG Representative: Sally Mui

Appendix 1: Domain Glossary

Term	Definition
Application	A system of software, hardware and data structure components that automate a business process. An application may be a single program, or consist of an entire group of interrelated databases, software programs, and hardware devices.
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system.
Authorization	Granting or denying access rights to a user, program or process.
Extranet	Expands technology of TCP/IP based networks that allow information to be shared by selectively making the information available to an organization, business partners, customers and suppliers.
Government Information Security Reform Act (GISRA)	The act primarily addresses the program management and evaluation aspects of security. It covers unclassified and national security systems and creates the same management framework for each.
Information Resources	This term encompasses both the information itself and the related resources; such as personnel, equipment, funds and information technology (A-130 and PRA) • **Information** 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. (A-130_ • **Information Technology** 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, including equipment used by a contractor under a contract that requires the significant use of such equipment to perform a service or furnish product. It includes computers, ancillary equipment software, firmware and similar procedures, services (including support services), and related resources. (PRA and Clinger-Cohen)
Integrity	The property that data has not been altered, either intentionally or accidentally, in an unauthorized manner; or the quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation.
Naming Conventions	A structure standard technique for identifying various entities to avoid confusion and disagreement.
Nonrepudiation	Provides proof of the origin or delivery of data • to protect the sender against a false denial by the recipient that the data has been received, or • to protect the recipient against false denial by the sender that the data has been sent.
Physical Security	The Security/Privacy Domain addresses physical security as it pertains to protecting RRB data and systems. It does not address the physical protection of

	the RRB building or employees.
Program	A structured list of instructions that, when executed, causes a computer to behave in a predetermined manner. It contains directions (called statements) telling the computer what to do with variables representing numeric data, text, graphical images, etc. There are many programming languages: C, C++, COBOL, BASIC, and Pascal are a few. Generally, a program performs an individual function within an application system.
System Development Life Cycle (SDLC)	Consists of the six phases needed to properly develop a system. These phases are: project definition, requirements definition, design, coding and testing, acceptance testing and implementation.
Security Profile	A set of characteristics related to security that varies for individuals, data and applications: • **Individual**: a set of privileges defining the extent to which (s)he may access and use data, programs, applications, systems and other information resource assets. • **Data**: a set of characteristics that describe the privacy and security needs for the data, including the data's sensitivity, who may access the data, and statutory or contractual restrictions on its use. • **Application:** the set of levels of authority built in to the application, each having particular capabilities to use the application. For example, a simple profile may have one level that authorizes viewing data, a second level for updating selected fields, and a third level for administering all aspects of the application.
User	Any person who uses an application to do work. The term includes RRB employees beneficiaries, and external partners.

Appendix 2: Conceptual to Domain Principle Matrix

	Relationship Between RRB's Domain Principles And Conceptual Architecture Principles																								
Domain Principle	***Conceptual Architecture Principles***																								
	CA 1	CA 2	CA 3	CA 4	CA 5	CA 6	CA 7	CA 8	CA 9	CA 10	CA 11	CA 12	CA 13	CA 14	CA 15	CA 16	CA 17	CA 18	CA 19	CA 20	CA 21	CA 22	CA 23	CA 24	CA 25
D-1		X																			X				
D-2		X																			X				
D-3				X																		X			
D-4					X						X			X							X				
D-5												X				X									
D-6															X										
D-7																X	X								
D-8																			X			X	X	X	
D-9																	X								

Conceptual Architecture Guiding Principles:

1. Use guidelines consistent with the Federal Enterprise Architecture. 2. Support a single Enterprise Wide Technical Architecture (EWTA). 3. IT projects are to be consistent with the Enterprise Architecture. 4. IT projects are to be consistent with the Enterprise Architecture. 5. Reduce integration complexity. 6. Technical architecture must be extensible and scalable. 7. Manage information and data as enterprise-wide assets. 8. Validate information as close to its source as possible. 9. Enhance the ability to capitalize on and exploit business information. 10. Support multiple data types. 11. Make an informed buy versus lease versus build decision before proceeding with any new development project. 12. Require shorter development cycle times. 13. Keep current with emerging technologies and their applicability to enterprise architecture. 14. Maximize infrastructure asset reuse. 15. Sustain reliable connectivity. 16. IT systems will be implemented in adherence with the agency's security, confidentiality and privacy policies. 17. The agency will use a consistent set of security interfaces and procedures. 18. Reduce total cost of operation (TCO). 19. Extend E-Mail to Become a Corporate Information Exchange Vehicle. 20. Adopt Open Systems Standards. 21. Reduce duplicate information systems. 22. Reduce duplicate information systems. 23. Maximize and exploit Internet and Intranet technologies and approaches. 24. Integrate Enterprise Architecture into the investment management process. 25. Customer perception is a measure of the quality of the automation processes.