FORM G-115f (1-92)

UNITED STATES GOVERNMENT

MEMORANDUM

RAILROAD RETIREMENT BOARD

June 15, 2009

L-2009-11

TO : Terri S. Morgan
Chief Information Officer

FROM : Steven A. Bartholow
General Counsel

SUBJECT : Classification of Contractor Systems Interacting with RRB's Information Systems

This is in reply to your memorandum dated May 8, 2009 wherein you requested a legal opinion regarding Contractor Systems that should be included in the Railroad Retirement Board's annual "FISMA" report to the Office of Management and Budget (OMB). Specifically, you asked whether a contractor system should be a reportable information system to OMB or if it should be considered to be a contracted service that is a function within the scope of an existing reportable information system of the agency. A brief review of the relevant statutory provisions and official guidance will be helpful in responding to your request.

FISMA is the Federal Information Security Management Act (FISMA), Title III of the E-Government Act of 2002 (Public Law 107-787, December 17, 2002). That law sets the policy for information security across the entire Executive Branch of government. FISMA requires federal departments and agencies to do the following:

- Maintain an inventory of information systems
- Perform periodic system risk assessments
- Implement policies and procedures to reduce risk to an acceptable level
- Periodically test and evaluate information security controls
- Provide appropriate information security training to employees and contractors
- Implement plans and procedures for security incident response and continuity of operations
- Report annually on information security status.

The reporting requirement is accomplished through an agency's annual "FISMA Report." Guidance to agencies for meeting their responsibilities under FISMA has been issued by OMB and by the National Institute of Standards and Technology (NIST).[1] Appendix III to OMB Circular No. A-130 defines the following terms that are used in this memorandum:

> "Application" means the use of information resources (information and information technology) to satisfy a specific set of user requirements.
>
> "Authorizing Official" is a senior management official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations, agency assets, or individuals.
>
> "General support system" or "system" means an interconnected set of information resources under the same direct management control which shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. A system can be, for example, a local area network (LAN) including smart terminals that supports a branch office, an agency-wide backbone, a communications network, a departmental data processing center including its operating system and utilities, a tactical radio network, or a shared information processing service organization (IPSO).
>
> "Major application" means an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Note: All Federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate.
>
> "Senior Agency Information Security Officer" is the agency official responsible for: (i) carrying out the Chief Information Officer responsibilities under FISMA; (ii) possessing professional qualifications, including training and experience, required to administer the information security program functions; (iii) having information security duties as that official's primary duty; and (iv)

[1] NIST is responsible under FISMA for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets.

heading an office with the mission and resources to assist in ensuring agency compliance with FISMA.

The Railroad Retirement Board (RRB) has a number of information systems provided by contractors. You asked whether a contractor system should be a reportable "information system" to OMB or if it should be considered to be a contracted service that is a function within the scope of an existing General Support System (GSS). If the contractor system is determined to be a reportable information system, then an independent Certification and Accreditation (C & A) is required as per OMB and FISMA and the contractor system must be reported as an information system for the agency on the FISMA report. If the contractor system is determined to be a contracted service within the scope of an existing GSS, then no separate entry must be made on the annual FISMA report and no separate C & A must be performed by the agency.

The National Institute of Standards and Technology (NIST) Special Publication 800-37 provides the guidance to federal agencies for implementing the provisions of FISMA related policies. Three key excerpts from 800-37 define an agency's authority to classify its own information systems:

> "The guidelines in the following sections are provided to assist agencies in defining information system boundaries to strike a balance between the costs and benefits of security certification and accreditation." (NIST 800-37 part 2.3)
>
> "Agencies have great flexibility in determining what constitutes an information system (i.e. major application or general support system) and the resulting security accreditation boundary that is associated with that system." (NIST 800-37 part 2.3)
>
> "It is quite possible for multiple information systems to be validly considered subsystems of a single, larger system provided all of these subsystems fall under the same higher management authority. This situation may arise in many agencies when other than major applications (i.e. minor applications) are coalesced for purposes of security certification and accreditation into a general support system. (NIST 800-37 part 2.3)

NIST 800-37 clearly gives discretion to an agency to determine for itself whether its contractor systems are a subsystem of a General Support System or not. The RRB has the responsibility to determine whether or not our various contractor systems are separately reportable and therefore require an independent C & A or whether a contractor system is properly secured through the RRB's own security protocols within the framework of an existing GSS.

The RRB has great latitude to determine how it will evaluate its own information systems and the security of those information systems. The authorities are clear, that categorizing information systems into GSS or subsystems is an agency level activity and that the RRB is supposed to take into account its own staffing and funding in making these determinations.

> "...establishing boundaries for agency information systems and the associated security certification and accreditation implications, is an agency-level activity that should include careful negotiation among key participants- taking into account the mission/business requirements of the agency, the technical considerations with respect to information security, and the programmatic costs to the agency." (NIST 800-37 part 2.3)
>
> "For large and complex information systems, the authorizing official and senior agency information security officer may define subsystem components with established subsystem boundaries.... This facilitates a more cost-effective certification and accreditation process by enabling scaling of the effort at the subsystem level in accordance with that subsystem's security category and allowing for reuse of certification results at the system level." (NIST 800-37 part 2.3)

These excerpts clearly indicate that the senior agency information security officer has the authority to define what constitutes a subsystem component of an overall information system or an overall GSS.

The practical application to the RRB is clear from the NIST guidance. The RRB, as an independent agency has the authority to define the boundaries of its own information systems. Within the RRB, the senior agency information security officer has the primary authority to analyze the security needs of the agency's information and define the boundaries of a GSS and whether or not contractor information systems operate as a part of the GSS or separate from a GSS. An important tool available to help make this last decision is the contract which was entered in order to acquire the contractor information system. The contract will describe what product and/or service is being provided and will include provisions that will indicate whether the product and/or service will operate as part of an existing GSS or as a separate GSS.

As an example, AT & T provides the web address or web site and the servers for RRB.gov. AT & T is clearly an integral part of RRB.gov, but RRB employees administer and control what information is placed on the web site. The overall system of the website is controlled or administered by RRB employees, even though AT & T provides the servers. It is an agency level decision on how to classify AT & T's contract system.

Questions to be addressed in making this decision would include the following:

Does providing the servers for a web site rise to the level of a GSS exclusively under the control of AT & T, or are the servers just a subsystem of the overall

GSS which is known as RRB.gov? The senior agency information security officer would also review the contract and obtain input from staff and other key participants.

The senior agency information security officer is in the best position to make information security evaluations to ensure the information security of the agency. It is my recommendation that the senior agency information security officer would also make the necessary classifications regarding contractor information systems. The senior information security officer should define each contractor system as either an independent information system and establish a Certification and Accreditation schedule for those systems or define each contractor system as a subsystem which functions as part of an overall General Support System. The latter finding would not require independent reporting on the annual FISMA report nor would it require independent Certification and Accreditation.

I:\wp7data\OPINIONS\FISMA K system(final).09.djb.doc
DJBartnicki:djb:etw:scm DJB
mpD