ERS Security Categorization and E-Authentication

Introduction

Employer Reporting System (ERS) Background

The Employer Reporting System (ERS) is a web-based system for use by employers covered under the Railroad Retirement and Railroad Unemployment Insurance Acts (the Acts) in exchanging information with the Railroad Retirement Board (RRB.)

Ultimately, the RRB will provide employers a paperless option(s) for filing forms with the RRB; receiving notices from the RRB; and receiving and replying to requests from the RRB. The web-based system will be provided to employers in addition to other media available for exchanging information with the RRB. The paper forms, systems, and processes that are currently being used to send and receive forms via other media will still be available. The existing legacy systems have their own security.

ERS includes a roles-based authorization access system, a Pin/password authentication system, a security tracking and tracing system, and an e-mail notification system. The roles-based access is determined for each application on the system based on whether the applicant's job duties (role) require access to that application.

The ERS system security will be evaluated using the guidelines established by NIST SP800-63. The ERS system will be part of the 'Employer Reporting' assessable unit and will be regularly tested and evaluated as part of that assessment.

What is in this report

This report is limited to issues of authentication. Authentication refers to establishing the identity of an individual and their validity to access ERS. This report begins with the determination of the required authentication assurance level for ERS based on a risk assessment. E-authentication consists of registration, identity proofing, and a token (in this case a password.) The report describes how each of these aspects meets the required assurance level. The report ends with a summary and list of references.

What is not included in this report

This document describes our confidence in the identity of the users of ERS. It does not address any security issues other than authentication. It should also be noted that the validation processing for the mainframe database is not part of this review. This edit-post processing is identical whether data is received via paper, magnetic cartridge, or web forms. Authentication of users of the web-based form DC-1 is not part of this discussion as that form resides on a separate web site and utilize authentication and access controls established by US Bank in conjunction with the US Treasury Department.

ERS Security Categorization

Assigning risk levels to potential breach of security

The FIPS Publication 199 defines three levels of potential impact on organizations or individuals should there be a breach of security; low, medium, and high risk. In general, the potential risk is low if the loss of confidentiality, integrity, or availability could be expected to have limited adverse effect on organizational operations, organizational assets, or individuals. For example, the RRB is able to perform its primary functions but the effectiveness of the functions may be (i) noticeably reduced; (ii) result in minor damage to organizational assets: (iii) result in minor financial loss; or (iv) result in minor harm to individuals. We assigned risk levels to ERS according to the guidelines in FIPS PUB 199. Details are in Attachment 1.

Potential impact of a breach of security

There are many checks and balances in the application process to prevent an unauthorized individual from receiving an ERS password. If, through human error or other means, an unauthorized individual or impersonator attains access to ERS, there is a low risk:

- that they will have access to private information;
- that the private information will cause distress to the private party;
- that civil or criminal violations will be enforced; or
- that the individual will cause financial loss to the agency.

See Attachment 1 for additional details.

Determining the required assurance level

The generally low risk levels indicate that ERS requires an assurance level 2 authentication. See the table in Attachment 1 for determination of the authentication level based on the risk level.

Assurance Level 2 Authentication

Level 2 authentication

The Executive Summary of NIST 800-63 states that 'Level 2 provides single factor remote network authentication. At Level 2, identity proofing requirements are introduced, requiring presentation of identifying materials or information.' A wide range of available authentication technologies can be employed at Level 2. It allows any of the token methods of Levels 3 or 4, as well as passwords. Successful authentication requires that the claimant prove through a secure authentication protocol that he or she controls the token. Eavesdropper, reply, and on-line guessing attacks are prevented.

We apply controls found in the 'ERS Administrator's Manual,' and the 'Form BA-12 Checklist,' to meet the level 2 authentication requirements. Form BA-12 Checklist is Attachment 2.

Registration requirements

Access to ERS begins with the filing of a paper application form, BA-12, *'Application for Employer Reporting Internet Access.'* The forms must be signed and certified by someone at the company who has signature authority and mailed to the RRB. When an application is received at the RRB, A&T reviews it and completes the "BA-12 Checklist" to validate the name of the certifying authority using existing RRB records. Once validated, a P/P is mailed to the applicant at the company's address of record. The application form and the completed checklist are stored in a secure area.

The ERS meets the registration NIST requirements for level 2 by maintaining records of the registration/application and by reviewing the applications according to written instructions. The RRB maintains a record of the actions taken to validate the application. Both documents are filed in a secure area.

Identity proofing requirements

The RRB meets the identity proofing requirements for level 2 by verifying information provided by the applicant on their application through record checks at RRB sufficient to identify a unique individual; by requiring that the application include the signature of a person known to the RRB; by requiring written signatures; and by mailing the Pin and Password to the address of record thus confirming the address.

The RRB's biggest advantage in authenticating an applicant/user is that there are less than 700 employers covered under the Acts and RRB staff has had personal contact with many of them. The RRB staff also have the following information available with which to validate an applicant.

- EDM contact official database;
- Form G-117a, Designation of Contact Official;
- Form G-440, Report Specification Sheet;
- correspondence;
- Pocket List of Railroad Officials; and
- seminar registration forms.

If anything is questionable, the RRB staff telephones an official contact at the company to validate the information on the application.

Assurance level 2 authentication

Level 2 authentication allows a wide range of available authentications, including passwords. If passwords are used, NIST PS 800-63 indicates that there should be protections against eavesdropper, replay, and on-line guessing attacks. RRB uses password encryption against eavesdroppers and replay.

Level 2 also requires that ERS administrators not reveal passwords to third parties. ERS passwords are encrypted and the encryption software is not available to any RRB staff. The software cannot be accessed even by RRB programming staff. Since no RRB staff has access to 1) unencrypted passwords, 2) the encryption algorithm, or 3) the software that creates and maintains the passwords, there is no possibility that RRB staff can disclose a password.

For level 2 protection against on-line guessing, NIST recommends "guessing entropy" of 30. Guessing entropy is an indication of the amount of work to determine, or guess, a password. Alternately, NIST indicates that any system that required passwords to be changed at least every two years and limited trials by locking an account for 24 hours after six failed attempts would satisfy the targeted guessing attack requirements for level 2.

ERS requires that passwords by changed every 90 days and will temporarily lock an account after three unsuccessful password attempts. An account is permanently locked after five unsuccessful attempts and can only be unlocked by a Password Administrator. ERS passwords must meet RRB password standards. It is determined that ERS passwords attained a "guessing entropy" of 30, as described in the next section.

Password rules and guessing entropy

We estimate that the ERS password system provides the 30 bits of "guessing entropy" recommended for level 2 in the NIST SP800-63, Appendix A. Entropy is the uncertainty of a value and "guessing entropy" is the difficulty in guessing the value or, in this case, the difficulty in guessing a password. ERS passwords meet the level 2 considerations as follows.

1. A minimum length of 8 characters, chosen by the user from an alphabet of 94 printable characters.

   ERS password length is 8 to 16 characters, chosen by the user from an alphabet of 70 characters. Several special characters are available for ERS passwords, but not every one. The variable password length which increases the difficulty in guessing a password offsets this limit.

2. Require passwords to include at least one upper case letter, one lower case letter, one number, and one special character.

   ERS passwords require three of the four. This limit is offset by the fact that after three unsuccessful attempts, a user is locked out for 60 minutes. This effectively prevents all automated password guessing.

3. Use a dictionary to prevent passwords from including common words and permutations of the username.

   ERS checks passwords against usernames and other common words and permutations.

The application form to gain access to the ERS system requires applicants to sign a statement that they will comply with the RRB's security guidelines. The guidelines are mailed with the application and are also found in the Reporting Instructions to Employers manual. The guidelines include practices for keeping your password secure.

Additional authentication strategies

The ERS meets the required level 2 authentication. In addition to the minimum requirements, the RRB has increased the level of assurance by applying mitigation strategies. The following are practices not mentioned elsewhere in this report which ERS uses to increase our assurance that only authorized users have access.

- A person in authority at the company must sign and certify the application form.
- Penalties for fraud are communicated on the application form (Form BA-12), written procedure (Reporting Instructions to Employers), and on the first web screen that appears when accessing the system.
- RRB system administrators perform daily monitoring of users accessing ERS. ERS captures a transaction record of activity processed and forms filed which includes the user's Logon ID, IP address, and browser information.
- A BA-4 Summary Report of ERS service and compensation data is created daily and made available to all users with BA-4 access at that company. This report is intended for use by employers to validate tax deposits and, as such, could detect an unauthorized user who obtained fraudulent access to file a report.
- The RRB requires that applications for access be mailed to the RRB. Using the United States Postal Service provides an additional deterrent against fraud.

Summary

Summary of determination	ERS meets the federal guidelines for authentication as indicated in OMB's E-Authentication Guidance for Federal Agencies, NIST's Special Publication 800-63, and FIPS Publication 199. ERS authentication is appropriate to the risk and cost. ERS security and authentication is in keeping with RRB's policy and guidelines. See Enterprise Architecture Strategy, by BIS 6/11/03.

List of Documents Referenced

NIST Special Publication 800-63, "Electronic Authentication Guideline" June 2004.
http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63v6_3_3.pdf

FIPS Publication 199 "Standards for Security Categorization of Federal Information and Information Systems" December 2003.
http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

OMB "Memorandum to the Heads of All Departments and Agencies" and Attachment A, "E-Authentication Guidance for Federal Agencies" (M-04-04) December 16, 2003.
http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdc

NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems (draft November 2004)
http://csrc.nist.gov/publications/drafts/SP800-53-Draft2nd.pdf

Risk Analysis to Determine the Required Assurance Level for Authentication

The first table shows the assurance levels assigned by OMB in their Attachment A of Memorandum to the Heads of All Departments and Agencies (M-04-04). The second table shows how ERS is rated in each of the six categories. Based on the assigned values for the six categories, ERS requires an Assurance Level 2 authentication.

	Assurance Level Impact Profiles			
Potential Impact Categories for Authentication Errors	**1**	**2**	**3**	**4**
1. Inconvenience, distress, or damage to standing or reputation	Low	Mod	Mod	High
2. Financial loss or agency liability	Low	Mod	Mod	High
3. Harm to agency programs or public interest	N/A	Low	Mod	High
4. Unauthorized release of sensitive information	N/A	Low	Mod	High
5. Personal safety	N/A	N/A	Low	Mod High
6. Civil or criminal violations	N/A	Low	Mod	High

Employer Reporting System (ERS)	**Assurance Level Impact Profiles**			
Potential Impact Categories for Authentication Errors	**1**	**2**	**3**	**4**
1. Inconvenience, distress, or damage to standing or reputation	Low			
2. Financial loss or agency liability	Low			
3. Harm to agency programs or public interest	N/A			
4. Unauthorized release of sensitive information		Low		
5. Personal safety	N/A			
6. Civil or criminal violations		Low		

The following descriptions of the potential harm or impact are taken from M-04-04. All levels are listed for comparison but the level assigned to ERS is in bold and a brief explanation follows the description. The risk from an unauthorized access takes into account not only the potential impact but also the likelihood of such impact.

1. Potential impact of inconvenience, distress, or damage to standing or reputation:
• **Low—**at worst, limited, short-term inconvenience, distress, or embarrassment to any party.

The impact is low because unauthorized access to ERS could not bring down ERS and could not yield access to any other system.

• Moderate—at worst, serious short term or limited long-term inconvenience, distress or damage to the standing or reputation of any party.

• High—severe or serious long-term inconvenience, distress or damage to the standing or reputation of any party (ordinarily reserved for situations with particularly severe effects or which affect many individuals).

2. Potential impact of financial loss or agency liability:

• **Low**—at worst, an insignificant or inconsequential unrecoverable financial loss to any party, or at worst, an insignificant or inconsequential agency liability.

The impact is low because if an unauthorized user gained access to ERS for the purpose of personal gain, there would be a very minimal amount of service and compensation (4 to 5 years) that could be added to an account without examiner review. The limited available information would yield a minimum financial loss to the agency in terms of erroneous RUIA benefits or an erroneous increase in RRA benefits. Such activity may be detected in various annual file comparisons and review operations in which case the erroneous benefits would be recovered.

• Moderate—at worst, a serious unrecoverable financial loss to any party, or a serious agency liability.

• High—severe or catastrophic unrecoverable financial loss to any party; or severe or catastrophic agency liability.

3. Potential impact of harm to agency programs or public interests:

N/A- We determined that this was not applicable because an unauthorized user cannot get from ERS to any other agency programs. (If we determined this to be low, the assurance level would still be 2.)

• Low—at worst, a limited adverse effect on organizational operations or assets, or public interests. Examples of limited adverse effects are: (i) mission capability degradation to the extent and duration that the organization is able to perform its primary functions with noticeably reduced effectiveness, or (ii) minor damage to organizational assets or public interests.

• Moderate—at worst, a serious adverse effect on organizational operations or assets, or public interests. Examples of serious adverse effects are: (i) significant mission capability degradation to the extent and duration that the organization is able to perform its primary functions with *significantly* reduced effectiveness; or (ii) significant damage to organizational assets or public interests.

• High—a severe or catastrophic adverse effect on organizational operations or assets, or public interests. Examples of severe or catastrophic effects are: (i) severe mission capability degradation or loss of to the extent and duration that the organization is unable to perform one or more of its primary functions; or (ii) major damage to organizational assets or public interests.

4. Potential impact of unauthorized release of sensitive information:

• **Low**—at worst, a limited release of personal, U.S. government sensitive, or commercially sensitive information to unauthorized parties resulting in a loss of

confidentiality with a low impact as defined in FIPS PUB 199.

The impact is low because an impersonator might potentially have access to personal information but only to a very limited amount. The exact information accessible depends on what information was available to the impersonated employer at that time. Information is further limited by ERS. For example, only seven years of service and compensation information is available to the BA-4 process.

• Moderate—at worst, a release of personal, U.S. government sensitive, or commercially sensitive information to unauthorized parties resulting in loss of confidentiality with a moderate impact as defined in FIPS PUB 199.
• High—a release of personal, U.S. government sensitive, or commercially sensitive information to unauthorized parties resulting in loss of confidentiality with a high impact as defined in FIPS PUB 199.

5. Potential impact to personal safety:
N/A- A breach of ERS security has no impact on personal safety.
• Low—at worst, minor injury not requiring medical treatment.
• Moderate—at worst, moderate risk of minor injury or limited risk of injury requiring medical treatment.
• High—a risk of serious injury or death.

6. The potential impact of civil or criminal violations is:
• **Low**—at worst, a risk of civil or criminal violations of a nature that would not ordinarily be subject to enforcement efforts.

The impact is low because civil or criminal violations are rare, particularly by employers, and are not ordinarily subject to enforcement efforts.

• Moderate—at worst, a risk of civil or criminal violations that may be subject to enforcement efforts.
• High—a risk of civil or criminal violations that are of special importance to enforcement programs.

BA _____

Form BA-12 Checklist

Action A&T	Initials-A&T	Date
1. Review form and check EDM records Is Form complete and properly signed? If anything is questionable, contact RRB supervisor for advice. (A question would arise if access is requested for an employer whose status is other than "R" reporting.) If requester is authorizer their own application, verify that the person is a designated contact official or certifying official (completes Forms G-440.) If not, inquire of the designated contact official concerning applicant. If requester is an EDM contact official, update any missing or revised data to EDM.		
2. Review requested access If access is approved, indicate "approved" or "OK as requested" in the "For RRB USE" section. Sign the BA-12 form as reviewer. If access is questionable, call the railroad to clarify. (Questions would arise if update access is requested for BA-4 but no one has approval access or if one type of contact official is requesting access completely outside their area.)		
3. Address an envelope Use the address on EDM. Use an envelope that says "Return after 5 days." Insert Getting Started instructions and Internet business card. (Replies to multiple applicants can be mailed together if they are mailed to the manager who approved all the applications.)		
4. Check ERS system for BA# If BA is on ERS, then initial here and deliver BA-12, checklist, and envelope to BIS Password Support section. If BA is not on ERS, then deliver material to System Administrator (SA). After adding the employer, the SA will initial and deliver material to BIS Password Support section.		
Action BIS	**Initials- BIS**	**Date**
5. Add requester to ERS system Assign and enter user ID and temporary password. Notate these on blue reply sheet and place in the envelope.		
6. Deliver envelope to mailroom Check that password sheet, Getting Started, and business card are included. Seal the envelope and deliver to the mailroom. Staple this checklist to the back of BA-12 form and deliver to Wayne Scharnak, 6th floor, to be filed by SA in secure area.		