

Note: an Interpretation cannot be used to change a standard.

Request for an Interpretation of a Reliability Standard
Date submitted: 9/14/2009
Date accepted: 9/18/2009
Contact information for person requesting the interpretation:
Name: Robert Ford
Organization: US Army Corps of Engineers
Telephone: 541-980-5160
E-mail: robert.w.ford@usace.army.mil
Identify the standard that needs clarification:
Standard Number: CIP-004-2
Standard Title: Cyber Security – Personnel and Training
Identify specifically what requirement needs clarification:
<p>Requirement Number and Text of Requirement:</p> <p>R3. Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access. A personnel risk assessment shall be conducted pursuant to that program within thirty days of such personnel being granted such access. Such program shall at a minimum include:</p> <p>R3.1. The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven year criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position.</p> <p>R3.2. The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.</p> <p>R3.3. The Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004.</p>
Clarification needed:
Question #1: What sources of verification (as alternatives to Social Security Number verification) are

acceptable? Would verification of a Driver's license, passport or birth certificate be acceptable under requirement R3.1?

Question #2: Is ID Verification required every seven years as stated in R3.2 for all situations or only in situations where an employee has a break in service or a name change?

Question #3: What is meant by the term "seven-year criminal check" in R3.1? Is a local or state check sufficient or is a national database required?

Identify the material impact associated with this interpretation:

Identify the material impact to your organization or others caused by the lack of clarity or an incorrect interpretation of this standard.

Failure to meet the Reliability Standard would put us at risk for fines/sanctions and over interpreting the requirement is a waste of valuable resources.

Project 2009-23: Response to Request for an Interpretation of Standard CIP-004-2 Requirement R3 for US Army Corps of Engineers

The following interpretation of CIP-004-2 – Cyber Security — Personnel & Training Requirement R3 was developed by the Cyber Security Order 706 SAR drafting team.

Requirement Number and Text of Requirement

R3. Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access. A personnel risk assessment shall be conducted pursuant to that program within thirty days of such personnel being granted such access. Such program shall at a minimum include:

R3.1. The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven year criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position.

R3.2. The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.

R3.3. The Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004.

Question #1

What sources of verification (as alternatives to Social Security Number verification) are acceptable? Would verification of a Driver's license, passport or birth certificate be acceptable under requirement R3.1?

Response to Question #1

The intent of identity verification is to ensure positive verification of an individual identity and that the risk assessment is performed on the same person who is being granted cyber or unescorted physical access. Each entity shall have a documented personnel risk assessment program that ensures each individual is positively identified.

The drafting team interprets that acceptable alternatives to the Social Security number verification are a current passport, driver's license, or identification (ID) card issued by a state or province or outlying possession of the United States; a Permanent Resident Card or Alien Registration Receipt Card; U.S., Mexican, or Canadian military ID card; or Native American tribal document or Certificate of Indian Status. ~~documents issued by a federal government agency that include an individual's photograph, name, and date of birth, such as a passport or military identification (ID) card. Additionally, a driver's license, state-issued ID card, or province-issued ID card would be acceptable.~~

Question #2

Is ID Verification required every seven years as stated in R3.2 for all situations or only in situations where an employee has a break in service or a name change?

Response to Question #2

The drafting team interprets that the personnel risk assessment (identity verification and criminal check) is required every seven years at a minimum. Requirement R3.1 states "The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven year criminal check." Since the wording of Requirement R3.1 does not make a distinction between the first and subsequent personnel risk assessments, the seven-year update requires both the identity verification and the seven-year criminal check.

Question #3

What is meant by the term "seven-year criminal check" in R3.1? Is a local or state check sufficient or is a national database required?

Response to Question #3

The drafting team acknowledges that the requirement does not define "seven year criminal check." The team interprets that due to the nature of cyber and unescorted physical access to critical facilities, the risk assessment must encompass a broad examination of an individual's record. Therefore, at least a "local agency check" should be performed. A local agency check is defined as a criminal history records check covering all locations where, during the period covered by the (re)investigation, the subject has resided, been employed, and/or attended school for six months or more, including current residence regardless of duration. ~~(normally understood to be through the city police department, county sheriff's department, or the state police) for every place of work and place of residence for the past seven years should be performed.~~