

**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
<b>Contact information for person requesting the interpretation:</b>	
Name:	Robert Ford
Organization:	US Army Corps of Engineers
Telephone:	541-980-5160
E-mail:	robert.w.ford@usace.army.mil
<b>Identify the standard that needs clarification:</b>	
Standard Number:	CIP-004-2
Standard Title:	Cyber Security – Personnel and Training
<b>Identify specifically what requirement needs clarification:</b>	
<b>Requirement Number and Text of Requirement:</b>	
<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.