Human Reliability Specialists since 1980

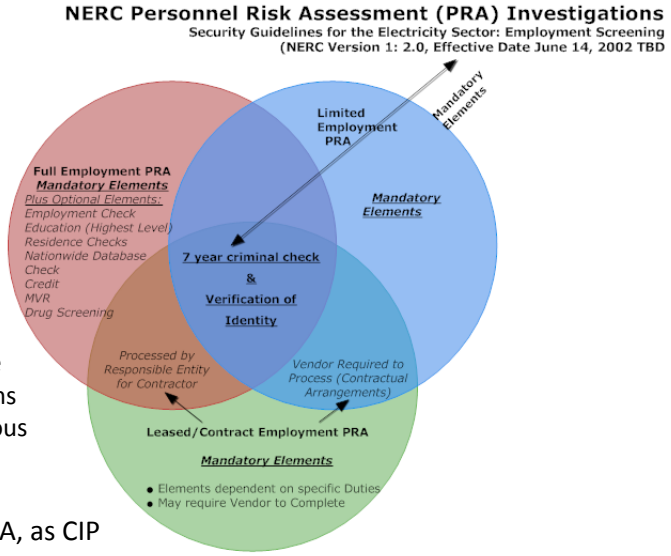
Volume 3, Issue 2, March 2013

CDI NEWSLETTER

NERC (North American Electric Reliability Corporation) Investigations

CDI NEWS: Electricity Sector

On January 24, 2011 the NERC Board of Trustees approved CIP-004-4. This CIP revision stated: "R3. Personnel Risk Assessment (PRA) – 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 to Critical Cyber Assets. A personnel risk assessment shall be conducted pursuant to that program prior to such personnel being granted such access except in specified circumstances such as an emergency. CIP-04-4 **mandates a 7 year criminal check and verification of true identity PRA** and a requirement to **update this every seven (7) years**. NERC past guidelines have suggested additional elements be considered depending on job classification or expected duties of the prospective employee. This is reflected in the graph below:



- **Full Employment PRA** – typically utilized for full time personnel working at or in support of critical facilities. Mandatory Elements plus expanded elements.
- **Limited Employment PRA** – appropriate for summer and intern students, co-op employees, and independent contractors who work at or in support of essential facilities on a brief or intermittent basis.
Mandatory Elements
- **Leased/Contract Employment PRA** – Specific duties would determine if more than mandatory elements are required. Lease and/or Contract PRAs may be required contractually with the vendor company.
- For applicants who are **non-citizens** or who have lived outside the country within the PRA time frame, full or limited background investigations may require international inquires including education, criminal and previous employer checks.

It is the company's discretion as to the extent or elements of the PRA, as CIP 04-4 specifically requires the following:

- 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-004-4."

On June 4, 2007 compliance with approved NERC CIP 004-4 Standards became mandatory and enforceable in the United States.

According to a December 8, 2010 NERC "Most Violated CIP Standards Webinar Series" one of the most violated standards

Volume 3, Issue 2, March 2013

CDI NEWSLETTER

Human Reliability Specialists since 1980

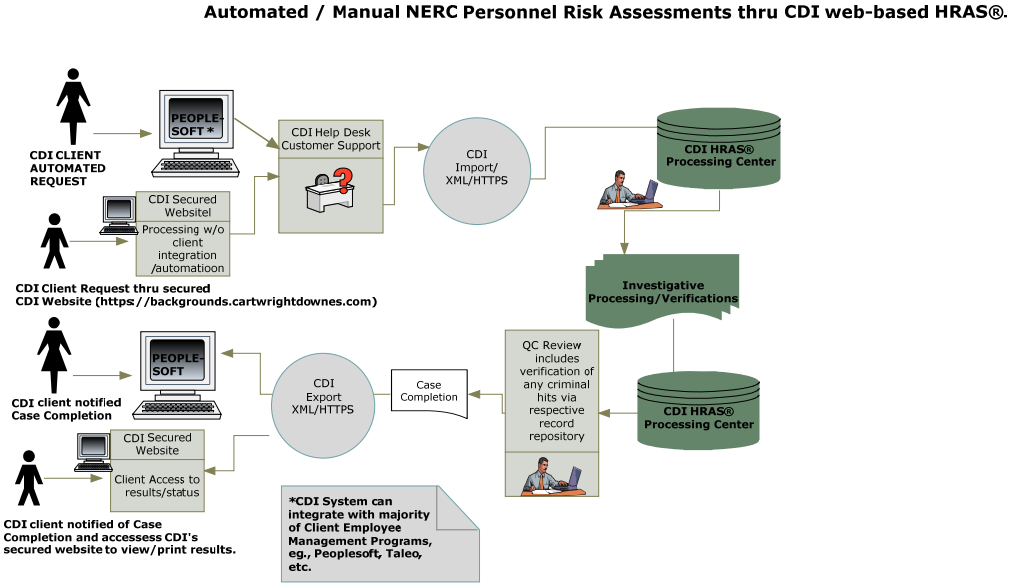
was **CIP 004 Personnel & Training**. The webinar identified 29 violations in this area and classified 25 of the reported 29 violations as: *"Risk Assessment – employees or contactors with access to critical cyber assets did not complete or had an incomplete background check (PRA), or was not updated within 7 years of the initial or for-cause PRA. Violations related to Responsible Entities as well as a number of contractors.*

- **NERC made the following recommendation**: "Entities need to ensure and verify that risk assessments on employees, contractors and service vendors with access to Critical Cyber Assets are not only completed within given time frames, but that the assessments focus on appropriate pieces of information."

Appropriate pieces of information (or the elements of the background investigation) are essentially left up to each Registered Entity. The CIP Standard in this area recognizes that the *"Registered Entity themselves are the experts on their systems and therefore are in the best position to define the overall strategy to best protect their systems."*

CDI offers a secured web-based system for processing and documenting Personnel Risk Assessments (PRAs) in a cost-effective, timely, qualitative and customizable fashion.

Sample Cost of CDI NERC Automated PRA Investigations Initial &/or 7 Year Criminal Re-Investigation:



NERC Mandatory Initial

- *7 YR LOCAL CRIMINAL Check* in jurisdiction of permanent residence. $15.00 + repository fee if any.
- *E-VERIFY*: Verification of social security number thru Social Security Administration. $6.00 (Clients have capability of processing said directly through SSA for no fee). E-Verify can only be utilized on client actual employees!
- *7 YEAR ENHANCED NATIONWIDE* includes database search of all available State Databases, identification of an aliases, search of all available government watch lists, search of all available sex offenders lists, trace and validation of social security number, and more. This is a database search producing same day results, however, if the search returns a criminal hit – a local repository search will be automatically requested to verify the accuracy of the information reported. $22.00
- *OTHER ELEMENTS* if required by client policy will be quoted upon request (eg, employment verification $14.00)