

*RDB received
01/15/05*

From: <grahamr@ritchie.disa.mil>
To: <rulemaking@nrc.gov>
Date: Mon, Feb 14, 2005 3:28 PM
Subject: Response from "Contact Us About Rulemaking-Ruleforum"

*12/16/04
69FR 75359
8*

Below is the result of your feedback form. It was submitted by
 (grahamr@ritchie.disa.mil) on Monday, February 14, 2005 at 15:27:55

comments: Comments on draft NRC Regulatory Guide DG-1130, Criteria for Use Of Computers in Safety Systems of Nuclear Power Plants.
 February 8, 2005

This review is submitted without access to the overall NRC documentation that controls the security of NRC systems assuming such exists. Access was likewise not available to IEEE standard 7-4.3.2-2003, Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations.

There should be overall structure for NRC computer systems that would also apply to safety systems. However, the safety systems would be considered mission critical and equivalent to DOD classified systems for the purpose of security controls (although the policy and criteria would not be classified). Overall structure can be developed by modifying and/or extracting from: OMB Circular A-130, Management of Federal Information Resources, DODD 8500.1, Information Assurance, DODI 8500.2, IA Implementation and CJCSM 6510.01 Defense-in-Depth: IA and Computer network Defense.

For example, DODI 8500.2 includes the following subject areas: security design and configuration, identification and authentication, enclave and computing environment, enclave boundary defense, physical and environmental, personnel, continuity, and vulnerability and incident management. In large part, information security is more than "something to be added to development"™, it is a concrete science with certification and accreditation of systems, rules for users and system administrators, access controls, encryption of sensitive traffic, vulnerability management, security certification and training of systems administrators, firewall and intrusion detection systems for network defense, continuity of operations (1) short-term (2) long-term recovery, etc. Could safety systems be operated from an external location in the event of an accident? This is just one continuity question.

DG-1130 references IEEE standard 7-4.3.2-2003, Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations. However, the standard is available only on a fee basis. This detracts from the usability of the information and does not promote the understanding of computer security. Also, the policy governing the use of computers in safety systems should have the IEEE standard as a part of the policy for easy reference.

Nuclear Power Generating Stations (NGPS) are part of America's™ critical infrastructure protection (CIP) program and this should be discussed in DG-1130.

Full scale risk assessments are no longer required by OMB. The IA community has adopted a series of security controls that provide a more concise and usable form of risk assessment. Given this comment, one risk assessment could be completed as a baseline for all NPGS computer safety systems. Controls could then be keyed on the results. Each NPGS would likely have some unique risks that must be mitigated by controls. Security controls are discussed in depth in DODI 8500.2.

DG-1130 is a difficult read for a non-engineer. If the audience of this document is not engineers, then the engineering slant of the document should be removed (e.g., rewritten by a non-engineer).

Paragraph number 2, section 4 says the QA organization should conduct periodic audits. This leaves too much room for interpretation. There should be a specific period.

*SISP Review Complete
 Template = ADM-013*

*E-RFDS = ADM-03
 Call = G. Aggarwal (SKA)
 P. Garrity (PA61)*

Paragraph 2.1, section 2, risk analysis requirement should be replaced with security controls and any site unique risks with mitigating controls. This relates to an earlier reference of security controls. Security controls are meaningful and clear and can be incorporated into a checklist.

Paragraph 2.1, section 3, DOD security guidance (e.g., DODD 8500.1, DODI 8500.2, CJCSM 6510.01) should be read and considered for DG-1130. Critical subject areas such as access controls and responsibilities should be discussed. In addition, remote access to Nuclear Plant safety software always involves an unacceptable threat and risk and should be prohibited.

Paragraph on Software code security reviews should be supported by vendor integrity statements.

Paragraph 2.2.1 section 1 "Recommend security controls be used to mitigate risk, see DODD 8500.2. Functional proponents and not developers should define security requirements with assistance and support from IA professionals.

Paragraph 2.2.1 section 3 and 2.3.1 section 2 "COTS poses a significant risk to Plant safety systems, COTS code should be reviewed prior to use, vendor integrity statements with penalties obtained and US developed COTS considered. If COTS cannot be effectively controlled, they should be forbidden. Also, section 3 isn't very clear and should be rewritten to include specific minimal COTS security requirements.

Paragraph 2.2.2 "Recommend that developers of Nuclear Plant safety software have some level of clearance or background investigation commensurate with the risks involved to plant personnel and the U.S. public.

Paragraph 2.3.1 section 3 "More detail and specificity is required regarding access controls. Perhaps Nuclear Plant safety systems should operate on a separate network.

To avoid repetition, comments concerning personnel, COTS, etc. extend from or cover systems concepts, requirements, design, implementation testing, installation, operations and maintenance. However, the maintenance area of the document has some good and unique guidance.

A management official must authorize in writing permission to operate a government system. The authorization is to be based on a minimum number of documents. This government requirement to authorize processing and related security requirements should be interwoven into DG-1130. These requirements cover both systems and the general support systems or enclaves where they operate.

Paragraph 2.4.2 provides a good recommendation to scan COTS code for malicious code. Unfortunately, code scans are not technically reliable in the case where significant risk is involved. If the NRC is really planning to attempt this, it will require considerable technical and monetary support.

DG-1130 is quite repetitive in the different life cycle phases. Repetition could be avoided by consolidating the like guidance of each phase.

name: robert graham

organization: submitting for the defense threat reduction agency

address1:

address2:

city: ft belvoir

state: VA

zip:

country: USA

phone: 703-915-1694

Mail Envelope Properties (421109DF.402 : 22 : 5122)

Subject: Response from "Contact Us About Rulemaking-Ruleforum"
Creation Date: Mon, Feb 14, 2005 3:27 PM
From: <grahamr@ritchie.disa.mil>
Created By: grahamr@ritchie.disa.mil

Recipients

nrc.gov
twf4_po.TWFN_DO
Rulemaking

Post Office
twf4_po.TWFN_DO

Route
nrc.gov

Files	Size	Date & Time
MESSAGE	6833	Monday, February 14, 2005 3:27 PM
Mime.822	7500	

Options

Expiration Date: None
Priority: Standard
Reply Requested: No
Return Notification: None

Concealed Subject: No
Security: Standard