NRCREP - comment for DRAFT REGULATORY GUIDE DG-5019

From: "sdportzline@netzero.com" <sdportzline@netzero.com>
To: <NRCREP@nrc.gov>
CC: <sdportzline@netzero.net>
Date: 09/02/2007 2:17:49 PM
Subject: comment for DRAFT REGULATORY GUIDE DG-5019

7/6/07
72FR37058
(2)

PLease add this to the public comment record for

DRAFT REGULATORY GUIDE DG-5019

There has been some troubles with the NRC's web pages for petition and comment submissions.

Scott Portzline

for TMI Alert

file atached

RECEIVED
2007 SEP -4 PM 2:06
RULES AND DIRECTIVES
BRANCH
USNRC

SUNSI Review Complete
Template = ADM-013

E-RIDS = ADM-03
Add = B. Schnetzler
(BAS5)

Mail Envelope Properties (46DAFE40.131 : 18 : 33073)

Subject:	comment for DRAFT REGULATORY GUIDE DG-5019
Creation Date	Sun, Sep 2, 2007 2:16 PM
From:	"sdportzline@netzero.com" <sdportzline@netzero.com>
Created By:	sdportzline@netzero.com

Recipients

nrc.gov
TWGWPO01.HQGWDO01
NRCREP

netzero.net
sdportzline CC

Post Office	**Route**
TWGWPO01.HQGWDO01	nrc.gov
	netzero.net

Files	**Size**	**Date & Time**
MESSAGE	216	Sunday, September 2, 2007 2:16 PM
TEXT.htm	290	
TMIALert comment DG-5019.pdf	44229	
Mime.822	63365	

Options

Expiration Date:	None
Priority:	Standard
ReplyRequested:	No
Return Notification:	None
Concealed Subject:	No
Security:	Standard

Junk Mail Handling Evaluation Results

Message is eligible for Junk Mail handling
This message was not classified as Junk Mail

Junk Mail settings when this message was delivered

Junk Mail handling disabled by User
Junk Mail handling disabled by Administrator
Junk List is not enabled
Junk Mail using personal address books is not enabled

August 31, 2007
Scott D. Portzline
3715 N 3rd Street
Harrisburg PA 17110

Rulemaking, Directives, and Editing Branch
Office of Administration
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

RE: DRAFT REGULATORY GUIDE DG-5019
(Proposed Revision 2 of Regulatory Guide 5.62, dated December 2006)
REPORTING OF SAFEGUARDS EVENTS

Secretary of the Commission Annette L. Vietti-Cook,

Please add these comments to record on behalf of Three Mile Island alert:

1. Concerning section 2.4 Examples of Security Events to be Reported Within 1 Hour

> "(3) The following are examples for interruption of normal operation of any NRC-licensed power reactor through unauthorized use of or tampering with its components, controls, or security systems:
> • tampering with plant equipment or physical security equipment that is either confirmed to be suspicious or malevolent in origin or is determined not to be reasonable mechanical failure or human error (Events which are suspicious in nature and for which no general assessment can be made within 1 hour, should be reported)
> • confirmed cyber attacks on or failures of computer systems that may adversely impact safety, security, and emergency preparedness
> • an actual or imminent strike by the security force"

We believe that licensees should report any "data storm" or network slowdown, whether it is understood, or whether the cause is undetermined, within 30 minutes of its

commencement. This would allow the NRC (and then in turn other federal law enforcement agencies and the Department of Homeland Security) to assess if there is a concerted cyber attack occurring at multiple reactor sites. Without such notification, a rapidly occurring trend may be overlooked and delay proper responses. Additionally, unaffected reactor sites could take additional temporary actions to secure their cyber systems until the threat is resolved.

The wording of the draft guide is too vague in its description of cyber system failures. For example: a slow down may not be considered a failure or even a safety concern. It may be considered normal. However, system attackers have created data storms as an opportunity to open portals to gain control of the system and issue commands.

Humans tend to delay conclusions that a serious computer problem exits. It is likely that systems managers will take remedial actions to recover control; including -- rebooting, replacing computer components, dumping data, seclusion, and simply "waiting it out." Because these responses could take hours, the licensee should be required to report that a cyber problem of unknown origin is occurring. It is too easy for licensees to create a "general assessment" (as per the draft guide) of an intermittent yet ordinary network slowdown.

Therefore, the wording for what conditions requiring cyber reporting must be clarified. The draft guide comes close but leaves too much "wiggle-room."

2. Although this following statement is not part of the proposed guide for reporting, we cannot understand why it is not already a safeguards requirement.

> "Licensee should consider obtaining access to NRC's Protected Webserver (PWS) in order to obtain routine threat bulletins and analyses from the Federal Bureau of Investigation (FBI) and U.S. Department of

Homeland Security (DHS). Licensee should contact region and headquarters staff for further information on obtaining access to PWS."

cyber crimes backgound:

• "In November 2006, the U.S.-China Economic and Security Review Commission reported that China is actively improving its nontraditional military capabilities.[1] According to the study, Chinese military strategists write openly about exploiting the vulnerabilities created by the U.S. military's reliance on advanced technologies and the extensive infrastructure used to conduct operations. Chinese military writings also refer to attacking key civilian targets such as financial systems. In addition, the report stated that Chinese intelligence services are capable of compromising the security of computer systems. The commission also provided instances of computer network penetrations coming from China. For example, in August and September 2006, attacks on computer systems of the Department of Commerce's Bureau of Industry and Security forced the bureau to replace hundreds of computers and lock down Internet access for one month."

• "In August 2006, a California man was convicted for conspiracy to intentionally cause damage to a protected computer and commit computer fraud. Between 2004 and 2005, he created and operated a botnet that was configured to constantly scan for and infect new computers. For example, in two weeks in February of 2005, the defendant's bots reported more than 2 million infections of more than 629,000 unique addresses (some infected repeatedly). It damaged hundreds of DOD computers worldwide. The DOD reported a total of $172,000 of damage due to a string of computer intrusions at numerous military installations in the United States (including Colorado, Florida, Hawaii, Maryland, South Carolina, and Texas) and around the world (including Germany and Italy). In addition, the botnet compromised computer systems at a Seattle hospital, including patient systems, and damaged more than 1,000 computers in a California school district over the course of several months in 2005. Officials from the California school district reported damages between $50,000 and $75,000 to repair its computers after the botnet struck in February 2005." [2]

• "The Central Intelligence Agency has identified two known terrorist organizations with the capability and greatest likelihood to use cyber attacks against our infrastructures." [3]

• "In March 2005, security consultants within the electric industry reported that hackers were targeting the U.S. electric power grid and had gained access to U.S. utilities' electronic control systems. Computer security specialists reported that, in a few cases, these intrusions had "caused an impact." While officials stated that hackers had not caused serious damage to the systems that

feed the nation's power grid, the constant threat of intrusion has heightened concerns that electric companies may not have adequately fortified their defenses against a potential catastrophic strike." [4]

[1] U.S.-China Economic and Security Review Commission, *2006 Report to Congress of the U.S.-China Economic and Security Review Commission* (Washington, D.C.: November 2006).

[2] DOJ, United States Attorney for the Western District of Washington, Press Release, *California Man Sentenced for "Botnet" Attack that Implicated Millions: Network of Robot Computers Damaged Military Installations, Northwest Hospital, and California School District* (Seattle, WA: Aug. 25, 2006).

[3] Statement for the Record, Information Operations Issue Manager, Central Intelligence Agency, before the Congressional Joint Economic Committee (Feb. 23, 2000). Page 21 GAO-07-705

[4] GAO, *Critical Infrastructure Protection: Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities*, GAO-05-434 (Washington, D.C.: May 26, 2005).

Scott D. Portzline
Security Consultant to Three Mile Island Alert