MANUAL

DOE M 470.4-1

Approved: 8-26-05
Review: 8-26-07
Chg 1: 3-7-06

SAFEGUARDS AND SECURITY PROGRAM PLANNING AND MANAGEMENT

U.S. DEPARTMENT OF ENERGY
Office of Security and Safety Performance Assurance

Vertical line denotes change.

AVAILABLE ONLINE AT:
http://www.directives.doe.gov

INITIATED BY:
Office of Security and Safety Performance Assurance

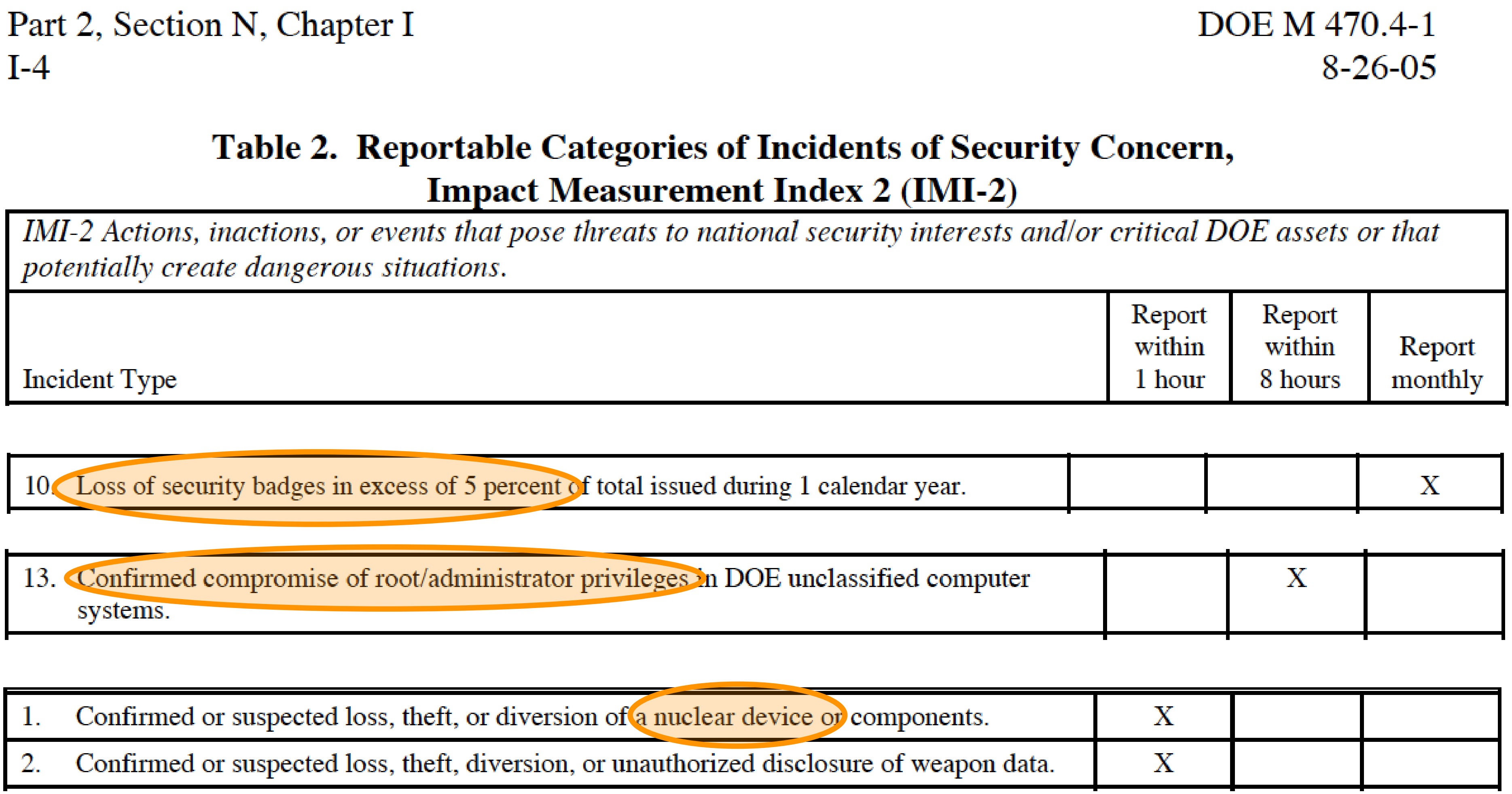
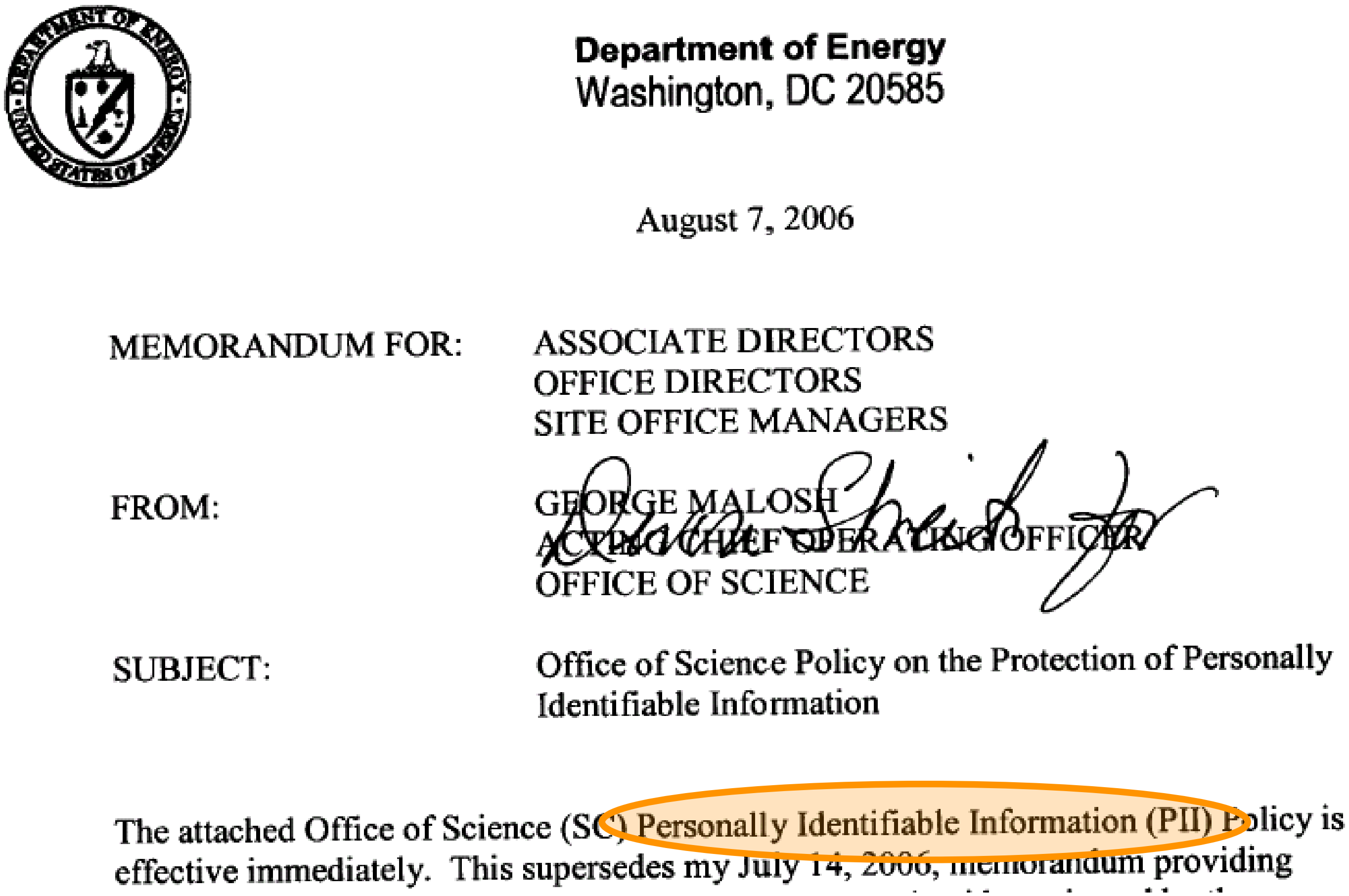


Table 2. Reportable Categories of Incidents of Security Concern, Impact Measurement Index 2 (IMI-2)

IMI-2 Actions, inactions, or events that pose threats to national security interests and/or critical DOE assets or that potentially create dangerous situations.

Incident Type	Report within 1 hour	Report within 8 hours	Report monthly
10. Loss of security badges in excess of 5 percent of total issued during 1 calendar year.			X
13. Confirmed compromise of root/administrator privileges in DOE unclassified computer systems.		X	
1. Confirmed or suspected loss, theft, or diversion of a nuclear device or components.	X		
2. Confirmed or suspected loss, theft, diversion, or unauthorized disclosure of weapon data.	X		



Department of Energy
Washington, DC 20585

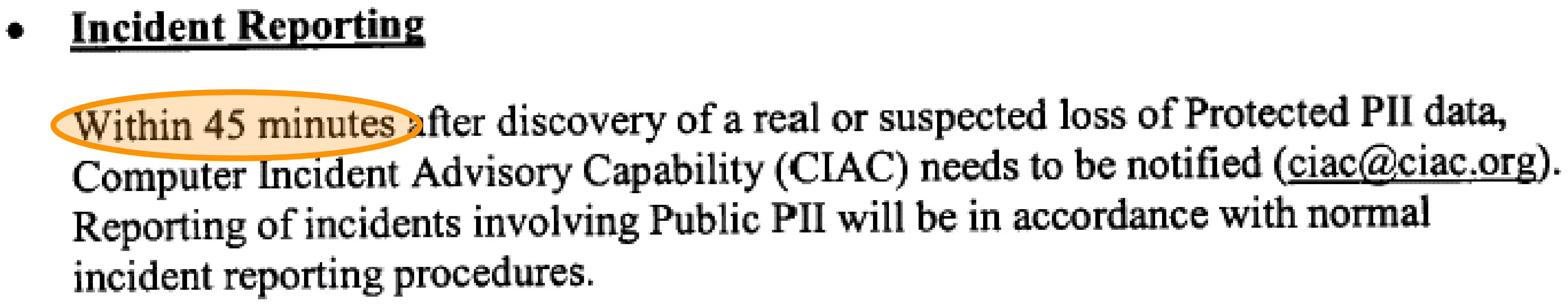
August 7, 2006

MEMORANDUM FOR: ASSOCIATE DIRECTORS
OFFICE DIRECTORS
SITE OFFICE MANAGERS

FROM: GEORGE MALOSH
ACTING CHIEF OPERATING OFFICER
OFFICE OF SCIENCE

SUBJECT: Office of Science Policy on the Protection of Personally Identifiable Information

The attached Office of Science (SC) Personally Identifiable Information (PII) Policy is effective immediately. This supersedes my July 14, 2006, memorandum providing



- **Incident Reporting**

  Within 45 minutes after discovery of a real or suspected loss of Protected PII data, Computer Incident Advisory Capability (CIAC) needs to be notified (ciac@ciac.org). Reporting of incidents involving Public PII will be in accordance with normal incident reporting procedures.

Sample *Snort* Signature

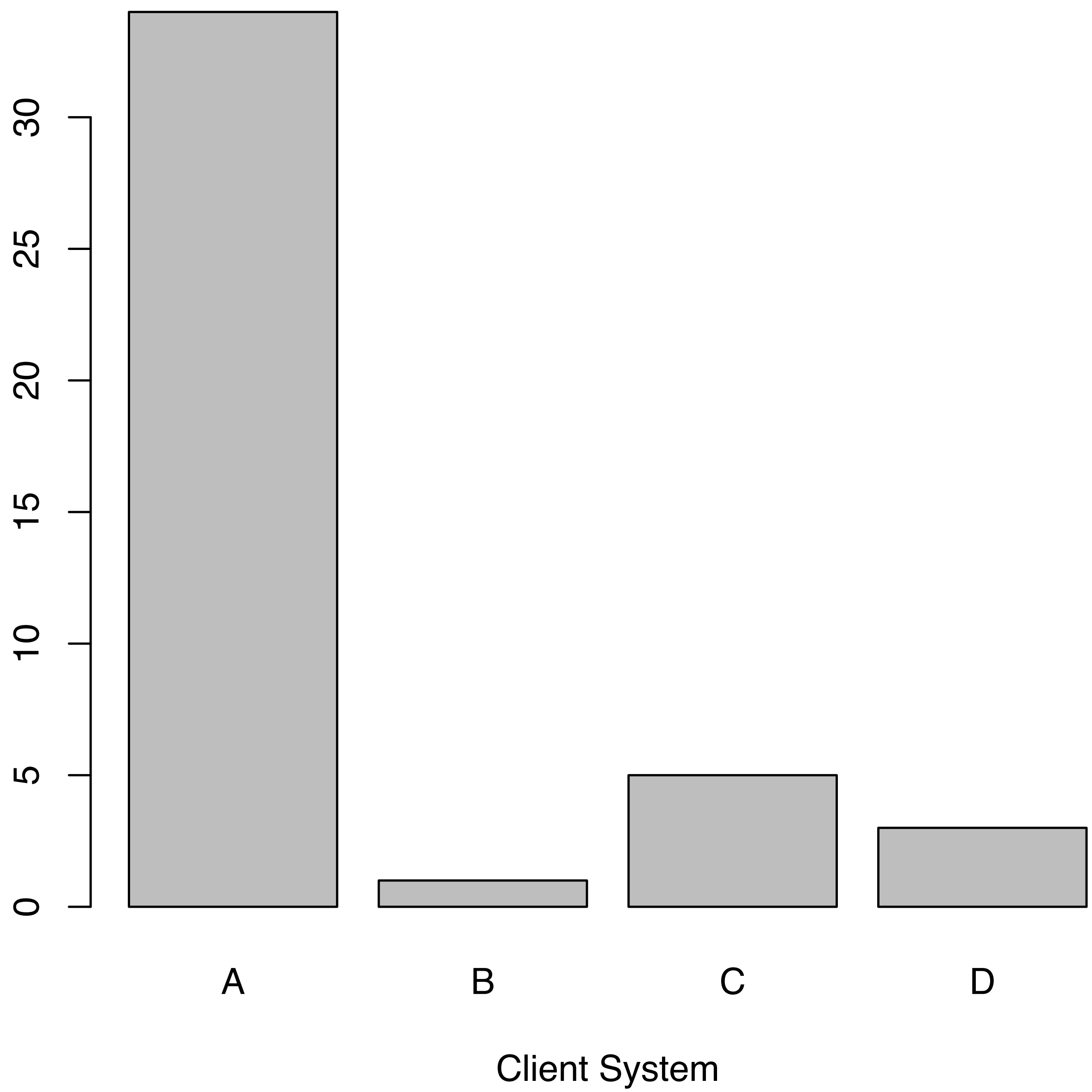
```
alert tcp $EXTERNAL_NET any ->
 $HOME_NET 139
 flow:to_server,established
content:"|eb2f 5feb 4a5e 89fb 893e
          89f2|"
msg:"EXPLOIT x86 linux samba overflow"
reference:bugtraq,1816
reference:cve,CVE-1999-0811
classtype:attempted-admin
```

Sample *Snort* Signature

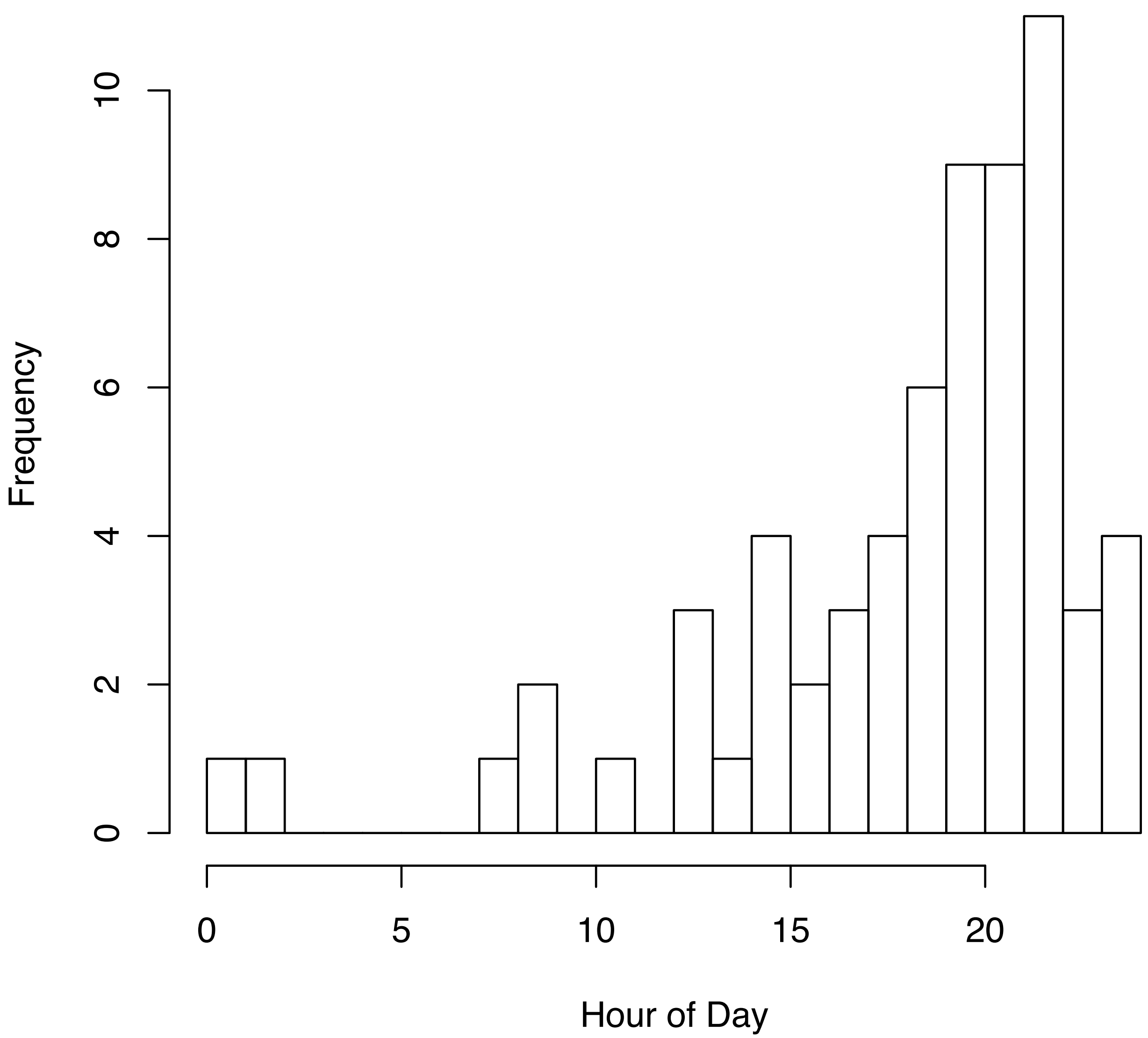
```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS
                               $HTTP_PORTS
    (msg:”ET Piranha default passwd attempt”;
    flow:to_server,established;
    uricontent:"/piranha/secure/control.php3”;
    content:"Authorization\: Basic
             cGlyYW5oYTp";
    reference:bugtraq,1148;
    reference:cve,2000-0248;
    reference:nessus,10381;
    classtype:attempted-recon;
    sid:2002331; rev:5;)
```

Sample Snort *Vulnerability* Signature

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS
                               $HTTP_PORTS
uricontent: ".ida?"; nocase; dsize: > 239;
 flags:A+
msg:"Web-IIS ISAPI .ida attempt"
reference:bugtraq,1816
reference:cve,CAN-2000-0071
classtype:attempted-admin
```



# Logins by User Joe to Machine Z



Hour of User Joe's Logins to Machine Z