Security Issues
DRAFT
June 23, 2003

1. Homeland Security Guidance

   Questions have been raised by science center directors and system administrators regarding how to adjust operations for the different Department of Homeland Security (DHS) threat advisory levels.

   To date, the DHS has provided no specific guidance for IT security that corresponds to the various threat levels. However, the Federal Computer Incident Response Center (FedCIRC) is a DHS agency that provides general computer security information online at – http:// www.fedcirc.gov/

   Scott McEwen's May 22, 2003 e-mail message (Subject: "Security Crystal Ball") provides a comprehensive list of actions to take during a high (orange) alert.

2. DMZ to Protect Public Access Hosts

   DOI has stated that any publicly accessed computer will have to be installed in a DMZ. Essentially, this means that any ftp server and web server will have to be segregated from science center local area networks by use of a firewall. Every publicly accessed computer has to have two firewalls between it and the public. DOI has granted the USGS to claim that one firewall may be a Cisco router with firewall software installed.

   It is still unclear as to whether or not servers accessed via ssh are to be considered as publicly accessible.

   USGS is going to have to show significant progress on consolidating web servers and ftp services in order to avoid buying hardware firewalls for every science center.

3. DOI/SAIC/KPMG Security Audit

   Jim Stapleton sent an update of the external DOI/SAIC scans on May 16, 2003 (Subject: "Status of USGS hosts reported on MAY SAIC scans"). This message was forwarded to WRD system administrators (SA's) and ITAC by Gary Neverdon on May 23, 2003. If any WRD computer was identified as being vulnerable, it wasn't obvious from Jim's summary. A very small percentage of the Bureau's computer systems were identified as being potentially vulnerable.

   Jim's letter mentions that security scans will begin soon from within the Bureau's firewall. Ideally, WRD SA's would be notified of the IP address (es) of the scanning computer(s) prior to the test, such that they aren't all reporting hacker incidents to the GIO's Incident Response Team (IRT) during the tests.

4. COO Plans

   All science centers should have prepared a Continuity of Operations (COO) plan for Y2K. A COO plan is a required document that details how a science center will react to an emergency situation in order to maintain service to the public. It includes such things as names and home phone numbers for people responsible for operating and/or recovering mission critical computer systems, databases, receivers, communications lines, and the like. It also includes information on alternate/emergency office locations and back-up systems.

   With the current administration placing more importance on security and potential threats, each science center will be required to update their COO plan in the near future. Guidance will be forthcoming from DOI.

5. SUS Server/Patches

   Currently, when a critical patch, recommended patch, or updated driver is made available by Microsoft (via http://windowsupdate.microsoft.com/) SA's download and install them on each workstation and server, as appropriate. Often, these patches exceed 10 MB each, and it isn't unusual for Microsoft to post one or more new patches

per week. Hence, downloading these patches to all science centers affects the Bureau's network performance by increasing traffic through the Internet portals.

In order to remove most patch-related traffic from the Bureau's Internet portals and wide-area network, Sam Martinez and Scott McEwen have proposed installing and managing Microsoft Software Update Services (SUS) servers in each region. The Central Region is currently testing the concept, and early results are promising. Tom Wood will give more details on this initiative at next week's meeting.

6. Web Resources

The best way for WRD science centers to ensure secure web services is to move their local web services to NatWeb, as per ITAC and Office of Information guidance.

7. Risk Assessments

Risk assessments are required documents for each mission critical system, and for each science center. As a result of the requirement to perform a risk assessment for mission critical systems, all SA's and NWIS database administrators (DBA's) are required to complete a risk assessment by July 15.

Additional guidance is expected for completion of office risk assessments.

8. NWIS Security Plan

This topic was discussed by Susan Trapanese and Richard Hollway at the June 10-12, 2003 Pennsylvania meeting.

9. Wireless Networks

Wireless local area networks (WLAN's) present a security challenge. Bureau guidance for securing WLAN's is in review, however, it is expected that DOI will institute a policy in the near future which forbids the use of WLAN's.

10. Identification of Security Teams & Personnel

The GIO's Office is still relatively new, and as such, is still being organized. There are currently two different groups within the GIO's Office tasked security responsibilities – the Bureau IT Security Manager's Office (BITSM) and the IT Security Operations Team (ITSOT). There's still a vacancy for the Bureau IT Security Manager.

The Bureau web pages related to security are woefully out of date.

Once the new BITSM Chief has reported for duty, it is expected that either the GIO or CTO will issue a memorandum explaining the responsibilities of each team. In time, the CTO should make sure that the Bureau security web pages reflect current issues and accurately identify security teams and personnel.