



GAO

Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

October 17, 2003

The Honorable Adam H. Putnam
Chairman, Subcommittee on Technology, Information
Policy, Intergovernmental Relations, and the Census
Committee on Government Reform
House of Representatives

Subject: *Posthearing Questions from the September 10, 2003, Hearing on Worm and Virus Defense: How Can We Protect Our Nation's Computers From These Serious Threats?*

As requested in your letter of September 15, 2003, this letter provides our responses to your questions for the record. At the subject hearing, we discussed effective patch management practices for mitigating the risks to critical information systems posed by exploits of vulnerabilities in widely used commercial software products.¹ We specifically discussed the Department of Homeland Security's (DHS) Patch Authentication and Dissemination Capability (PADC). PADC is a service offered by DHS's Federal Computer Incident Response Center (FedCIRC) that provides federal agencies with information on trusted, authenticated patches for their specific technologies without charge. Your questions, along with our responses, follow.

1. According to your testimony, FedCIRC offers a free service for agencies that offers validated, tested patches, but agencies are not utilizing this service. Why do you think utilization is so low? Should OMB require that all agencies use PADC?

The Director of FedCIRC reported that as of September 10, 2003, 47 agencies subscribed to PADC. However, the Office of Management and Budget (OMB) has reported that while many agencies have established PADC accounts, actual usage of these accounts is extremely low. Because we have not reviewed subscribing agencies' utilization of the PADC service, we cannot determine the extent to which it is being utilized.

Nevertheless, FedCIRC officials have acknowledged limitations to the PADC service, specifically regarding the number of subscriber accounts and the level of services currently provided. Due to monetary constraints, only about 2,000 accounts are available throughout the federal government. According to officials from agencies with whom we spoke regarding their potential subscription to the PADC service, the number of accounts that FedCIRC can offer them is not adequate to serve their entire agency. Moreover, other patch management tools and services are available that offer greater capabilities and functionality, including tools that are designed to be stand-alone patch management systems, that can deploy patches across agency networks, and that can verify that patches have been successfully installed.

¹ U.S. General Accounting Office, *Information Security: Effective Patch Management is Critical to Mitigating Software Vulnerabilities*, GAO-03-1138T (Washington, D.C.: September 10, 2003).

Because of PADC's limitations, an official from one of the agencies with whom we discussed PADC told us that his agency has decided not to subscribe to the free service and, instead, use other methods and tools to perform patch management. As mentioned in our testimony, DHS is considering broadening the scope of PADC's capabilities and increasing the number of user accounts.

To comply with the Federal Information Security Management Act (FISMA), OMB requires that each agency develop specific system configuration requirements that meet its own needs and ensure compliance with them. This provision encompasses traditional system configuration management, employing clearly defined system security settings, and maintaining up-to-date patches. OMB further states that simply establishing such configuration requirements is not enough; adequate ongoing monitoring and maintenance must also be implemented.

As discussed above, PADC is but one of a variety of available services and automated tools, and does not include important features that are available in other services and products. Agencies should examine these tools and services and implement the most cost-effective solution available for their computing environment. In considering whether to require agencies to use the PADC service, OMB should weigh the costs against potential benefits, considering the possible changes in PADC scope and user base discussed above.

2. We know from the hearing on the 2002 GISRA report that most agencies do not have a complete inventory of their systems. In the absence of a complete inventory, is it possible to have effective patch management?

Without a complete inventory of systems, it is very difficult to implement effective patch management agencywide. In our testimony we specifically identified the practice of creating and maintaining a current inventory of all hardware equipment, software packages, services, and other technologies installed and used by an organization as an essential element of patch management. A systems inventory assists in determining the number of systems that are vulnerable and require remediation, in locating the systems and identifying their owners, and in prioritizing systems to be patched based on a risk assessment. The National Institute of Standards and Technology's (NIST) Special Publication 800-40, *Procedures for Handling Security Patches*, also identifies a systems inventory requirement as a key priority for effective patch management. According to NIST, it is important for the inventory to include hardware, operating systems, and major applications. Systems administrators may be able to keep patches up to date on their individual systems without an agencywide inventory, but this option may be riskier, less consistent, and more expensive.

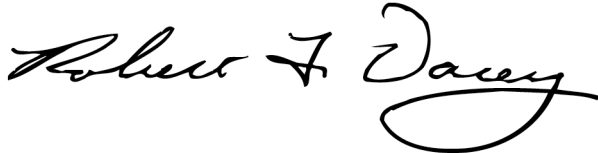
3. Several panelists suggested that the federal government should have security acceptance testing for software prior to purchasing. What are your thoughts on this idea?

As part of the acquisition decision process, agencies should test software to ensure that it meets their security requirements before purchasing it. OMB requires agencies to use a certification and accreditation process to ensure that a new system meets a set of specified security requirements before it is deployed. Moreover, NIST's Special Publication 800-23, *Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products*, includes guidance advising agencies of the benefits of testing

commercial products against customer-, government-, or vendor-developed specifications. Typically these specifications include security requirements.

We are sending copies of this letter to DHS and other interested parties. Should you have any questions on matters discussed in this letter, please contact me at (202) 512-3317. I can also be reached by e-mail at daceyr@gao.gov.

Sincerely yours,

A handwritten signature in black ink that reads "Robert F. Dacey". The signature is written in a cursive style with a large, looping flourish at the end of the name.

Robert F. Dacey
Director, Information Security Issues