



FEB 6 2009

TO: Distribution

FROM: Deputy Chief Information Officer for IT Security

SUBJECT: FY 2009 Scanning and Vulnerability Elimination or Mitigation

This memorandum establishes new, minimum vulnerability scanning requirements; all Centers and Programs are strongly encouraged to establish more stringent and frequent scanning practices. Vulnerability scans are an essential tool for identifying and correcting vulnerabilities. Strong control measures need to be put in place to ensure that all NASA systems are scanned on a recurring basis. This requirement will be met in conjunction with any Center specific policy related to scanning and patching.

All network devices found on NASA networks and NASA devices on other networks must be scanned, at minimum, monthly for all high vulnerabilities using the McAfee Foundstone vulnerability scanning tool. The vulnerability severity is set by software vendors and found within Foundstone. The monthly scan completion date will follow the ASUS Non-waived patch reporting schedule as defined in https://patches.ksc.nasa.gov/files/reporting/Reporting_Schedule.pdf

To support NASA's goal of vulnerability reduction, all Centers and Programs shall allow the NASA IT Vulnerability Scanning Project Manager or designee access to the Foundstone scanner data. This data will be used to generate Agency and Center vulnerability reports. The purpose of these reports is to provide NASA and Center management with information demonstrating assurance that the full IP address space is being scanned regularly and vulnerabilities are being detected and mitigated in a timely fashion.

Each Center shall run an appropriate version of the Foundstone scanner tool as set by the NASA IT Vulnerability Scanning Project Manager with vulnerability definitions no older than 30 days. Centers will also consolidate all production Foundstone databases into a primary database and allow the NASA IT Vulnerability Scanning project to install a McAfee provided data synchronization module which will push data from the Center's primary Foundstone database to an Agency data warehouse.

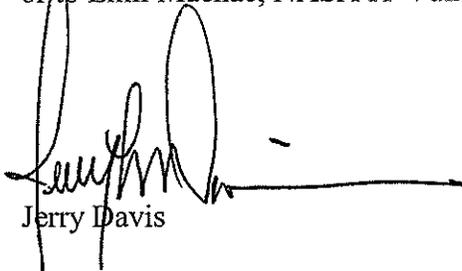
System Owners are responsible for eliminating or mitigating all known high-risk vulnerabilities, at minimum, and for ensuring that previously identified vulnerabilities

continue to be mitigated. To do this effectively, System Owners must maintain an accurate inventory of all devices that are part of their information system (this is also a requirement of the system security authorization process, or C&A). A device identification process is being developed for Agency-wide use.

Any device found on NASA networks and NASA devices on other networks that continue to exhibit the same vulnerabilities identified in three consecutive monthly scans must be disconnected from the network, and only re-connected once all these vulnerabilities are eliminated or mitigated. Centers may choose to disconnect these devices sooner depending on the severity of the vulnerability or sensitivity of the device.

For systems with a vulnerability for which no mitigation strategies are available, the system owner must document the vulnerability and risk in the system's Plan of Actions and Milestones (POA&M) with the authorizing official's approval and notification to the Center ITSM. If a system cannot meet the requirements of this memo due to a flight freeze or other mission critical reason, the Information System Owner must follow the NASA IT Waiver Process. Please refer to the NASA IT Waiver in Appendix A for further guidance on obtaining a waiver.

Questions concerning this scanning requirement should be directed to me at (202) 358-1401 or to Emil Machac, NASA IT Vulnerability Scanning Project Manager at (661) 276-6135.

A handwritten signature in black ink, appearing to read "Jerry Davis", with a long horizontal line extending to the right from the end of the signature.

Jerry Davis

Enclosure

DISTRIBUTION:

Center CIOs:

ARC/Christopher Kemp
DFRC/Robert Binkley
GRC/Dr. Sasi Pillay
GSFC/Linda Cureton
HQ/Kelly Carter (Acting)
JPL/Jim Rinaldi
JSC/Larry Sweet
KSC/Mike Bolger
LaRC/Cathy Mangum
MSFC/Jonathan Pettus
NSSC/Ken Griffey
SSC/Gay Irby

cc:

Center ITSMs:

ARC/ Ernest Lopez
DFRC/Larry Johnson
GRC/Don Cannatti
GSFC/Joshua Krage
HQ/Greg Kerr
JPL/Jay Brar
JSC/Ted Dyson
KSC/Henry Yu
LaRC/Kendall Freeman
MSFC/Walter Franklin
SSC/Christine Reynolds
NSSC/James Cluff

Enclosure

NASA Information Technology (IT) Waiver Process December 2008

Waivers to Information Technology (IT) Policies, Procedures, Standards, or Federal Requirements

1. Waivers to IT policies, procedures, standards or requirements standards, shall be granted by the NASA CIO.
2. The NASA CIO may delegate authority and responsibility to Center CIOs for a specific type of IT waiver or for a specific program or issue.
 - 2.1. The NASA CIO delegation of waiver authority and responsibility shall be in writing for the specific delegated authority or be as specified in NASA policy directives, e.g. in an NPR.
3. The individual/office preparing the waiver request shall submit the waiver request to the cognizant Center CIO for Center CIO concurrence and action. Example: The Sounding Rocket Program at the Wallops Flight Facility would submit the waiver to the GFSC CIO for review and concurrence/non-concurrence.
4. The waiver request shall include:
 - 4.1 The NASA IT policy, procedure, standard, and/or Federal requirement to be waived.
 - 4.2 The reason and justification for the waiver is required including:
 - a. Risk Assessment;
 - b. Cost-Benefit Analysis;
 - c. Business Impact Assessment;
 - d. Identification of compensating controls/actions;
 - e. Proposed period of time for the waiver;
 - f. The proposed date by which the Center will be compliant with the NASA IT standard, security control, and/or Federal requirement; and
 - g. For an IT security control waiver or for any waiver that results in an unmitigated security weakness or deficiency, an Authorization Official (AO) approved Program of Action and Milestone (POA&M) shall be included with the waiver request.
5. The Center CIO shall evaluate the waiver and either concur or non-concur within 30 calendar days of receipt.
 - a. Non-concurred waivers shall be returned to the requester.
 - b. Non-concurred waivers may be escalated to the Center Director or designee.
6. The Center CIO will forward the waivers with concurrence to the NASA CIO.
7. The NASA CIO shall evaluate the waiver request and the Center concurrence and either approve or disapprove the request within 30 calendar days of receipt.

8. For waivers to requirements contained in NASA policy documents, this waiver process applies only to those policy documents for which the Office of the CIO is responsible. For waivers to requirements in NASA policy documents for which the NASA CIO is not responsible, the requester shall follow the waiver process called out in the NASA policy document itself.