

National Aeronautics and
Space Administration
Office of the Administrator
Washington, DC 20546-0001



October 2, 2007

NPS 1600.99
NID 1600.55

TO: Officials-in-Charge of Headquarters Offices
Directors, NASA Centers

FROM: Deputy Administrator

SUBJECT: Safeguarding Sensitive but Unclassified Information

All NASA employees are covered by this memorandum, and it contains important information on each employee's responsibilities and obligations. I encourage you to read the attachment carefully and request that you disseminate the message to your employees.

A handwritten signature in black ink, appearing to be "Shana Dale".

Shana Dale

Enclosure **W 1400-8**
NID 1600-54
NPR 1600.1
NRW 1600-34
NRW 1400-48

Safeguarding Sensitive but Unclassified Information

Point of Contact: Steve Peyton, Information Security Program Manager, Office of Security and Program Protection, (202) 358-0191

Note: Everyone is covered by this memorandum, and it contains important information on each employee's responsibilities and obligations. I encourage you to read it carefully and request you disseminate the message to your employees.

Background

NASA generates, receives, disseminates, and maintains an enormous amount of information, much of which is of an unclassified/nonsensitive nature with few restrictions on its use and dissemination. In special cases, however, NASA employees and contractors may have access to information that is considered sensitive but unclassified (SBU) and in such cases every employee has an ongoing obligation to protect that SBU information against inappropriate access and disclosure. Given the rapid advances in information technology capabilities and the ability for an individual to almost instantaneously send vast amounts of information globally, it is imperative that all NASA employees have a clear understanding of the procedures related to the safe handling of SBU information. To address this important issue, Section 5.24 of the existing NASA Procedural Requirements (NPR) 1600.1, NASA Security Program Procedural Documents, will soon be updated to clarify the designation and safeguarding of SBU information at NASA and your responsibilities, under both law and policy, to appropriately safeguard SBU information.

Notice

As I stated, designation of SBU within NASA is currently being updated. In the interim, I want to emphasize, in particular, that each employee is responsible for protecting privacy, proprietary, procurement-sensitive, and export-controlled information. In addition to the civil and criminal penalties noted below, employees will be subject to administrative and/or disciplinary action, up to and including removal.

Training

To ensure a thorough understanding of your many responsibilities related to the handling of SBU information, all employees are required to complete mandatory SBU training by November 30, 2007. Each Center Protective Services Office will advise employees on how to complete training through SATERN.

Enclosure

In view of this Agency training requirement, and recent direction from the White House Office of Management and Budget regarding "*Safeguarding Against and Responding to the Breach of Personally Identifiable Information*,"

<http://www.whitehouse.gov/omb/memoranda/index.html>, I want to personally emphasize the importance of safeguarding SBU information, and the potential penalties for not doing so. Safeguarding SBU information in the possession of the Government and preventing its breach are essential to ensure that the Government retains the trust of the American public. You can anticipate future updates on this issue as current efforts are under way at NASA, and by a U.S. Government-wide task force group, to further address protection of SBU Information.

Statutory Prohibitions on Disclosure of SBU

Information required to be protected by statute or pursuant to an agreement with the owner of the information must be designated as SBU. The following types of SBU are most frequently encountered at NASA:

- **Information protected by the Privacy Act.** All employees are reminded of their specific responsibilities for safeguarding personally identifiable information (PII) and that willfully disclosing it to those not entitled to receive it may subject an employee or contractor to criminal prosecution and/or fine. 5 U.S.C. §552a.
http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=browse_usc&docid=Cite:+5USC552a
- **Information protected by the Trade Secrets Act.** Government employees are subject to criminal prosecution and removal from office for wrongful disclosure of information protected by the Trade Secrets Act. NASA employees may only disclose proprietary information received in the course of government employment to individuals who are authorized to receive the information, or as otherwise authorized by law. 18 U.S.C. §1905.
<http://www.nasa.gov/offices/ogc/commercial/18usc1905.html>
- **Information protected by the Procurement Integrity Act.** Employees may not knowingly disclose contractor bid or proposal information or source selection information. 41 U.S.C. § 423.
http://www4.law.cornell.edu/uscode/html/uscode41/usc_sec_41_00000423----000-.html
- **Export Controlled Information.** In addition, if information is determined to be export controlled (i.e., export is restricted or prohibited) under the International Traffic in Arms Regulations (ITAR) or Export Administration Regulations (EAR), it must be protected from inappropriate disclosure to foreign entities. Revealing such ITAR or EAR information, for example in a public speech or research paper or other public forum, or placing information on a Website without an export license is a

violation of export control laws, for which civil and criminal penalties can be imposed. NPR 2190.1.

<http://nodis3.gsfc.nasa.gov/displayDir.cfm?t=NPD&c=2190&s=1A>.

- **Other sensitive information not specifically marked as SBU.** Even when materials have not been specifically marked as SBU, but nonetheless contain sensitive information, public disclosure should be avoided. An employee's unwarranted disclosure of sensitive information acquired in the course of Government employment demonstrates a lack of sound judgment and a breach of the trust and confidence that NASA has placed in that employee. Supervisors may consider an employee's lack of judgment or breach of confidence during the performance appraisal process and may also subject the employee to disciplinary action when warranted.

NASA greatly values the free exchange of ideas among employees and the scientific community. NASA further supports the rights of employees to exercise their rights under the Whistleblower Protection Act, 5 U.S.C. § 1213. <http://uscode.house.gov/uscode-cgi/fastweb.exe?getdoc+uscview+t05t08+133+1++%28%29> AN. Nevertheless, employees have not only a legal but also an ethical responsibility not to disclose SBU information to unauthorized personnel. Executive Order 12674 "*Principles of Ethical Conduct for Government Officers and Employees*."

http://www.usoge.gov/pages/laws_regs_fedreg_stats/lrfs_files/exeorders/eo12674.html

This memorandum reemphasizes your responsibilities under law and NASA policy.