




Homeland Security

January 11, 2005

TO: Under Secretaries
General Counsel
Chief of Staff
Executive Secretary
Commandant, U.S. Coast Guard
Director, U.S. Citizenship and Immigration Services
Director, U.S. Secret Service
Director, Office of State and Local Government
Coordination and Preparedness
Director, Federal Law Enforcement Training Center
Assistant Secretary for Public Affairs
Assistant Secretary for Legislative Affairs
Commissioner, U.S. Customs and Border Protection
Assistant Secretary, U.S. Immigration and Customs
Enforcement
Assistant Secretary, Transportation Security Administration

FROM: Janet Hale, 
Under Secretary for Management

SUBJECT: Management Directive 11042.1, "*Safeguarding Sensitive but
Unclassified (For Official Use Only) Information*"

DHS is uniquely situated due to its mission to protect the nation's homeland and infrastructure. As a result, DHS employees are entrusted with vast amounts of sensitive but unclassified (SBU) information every day, and regularly and rightfully share it with other Federal agencies and our partners in state and local governments, tribal officials, and the private-sector. Examples of these types of information include:

- Vulnerability assessments of the nation's critical infrastructure, including Protected Critical Infrastructure Information (PCII), e.g., bridges and tunnels, pipelines for hazardous/flammable liquids, air-traffic equipment, and government buildings;
- Information technology systems servicing these critical infrastructure facilities;

- Strategic and tactical law enforcement plans, capabilities, operations, and investigative techniques, methods, and sources;
- Research and development of sensitive technology, including proprietary information, as well as information about devices to detect chemical, biological or other destructive weaponry; and
- Information that could endanger the physical security and safety of DHS employees.

Protecting this SBU information is therefore an essential element of ensuring the nation's homeland security as is sharing it with those that need it. To safeguard this information without impeding its legitimate flow, DHS established Management Directive (MD) 11042 "Safeguarding Sensitive but Unclassified (For Official Use Only) Information" in May 2004. This policy was created in order to define for our employees what constitutes SBU information and provide standards to safeguard it. Included in this initial policy was a requirement to execute a Non-Disclosure Agreement (NDA) for access to SBU information. This provision was designed as an interim measure to efficiently and effectively educate employees and communicate the standards promulgated by the MD.

Effective January 6, 2005, MD 11042 has been superseded by revised version MD 11042.1 that expands upon and formalizes its educational purpose without the need for our employees or Federal detailees to complete an NDA. Pursuant to the revised policy, the DHS Office of Security will develop and implement an education and awareness program for the safeguarding of SBU information. Once this program is developed and appropriate notifications are provided, all employees will participate in classroom or computer-based training sessions designed to educate employees on what constitutes SBU information and the standards for handling and disseminating it. Completion of this training will ensure that each employee has the knowledge they need to recognize and handle SBU information responsibly.

Those NDA's previously signed by DHS employees pursuant to MD 11042 will no longer be valid. The Office of Security in a subsequent communication will provide instructions for the proper collection of these documents. DHS will take reasonable steps to retrieve these documents and destroy them in accordance with DHS records management policy. All employees, however, are reminded that they are obligated to follow the statutory and regulatory requirements governing the handling and dissemination of all categories of SBU information.

MD 11042.1 is available online at www.dhsonline.dhs.gov.