These documents were posted as part of the Categorical Exclusions Detailed Administrative Record and the Other Supporting Information. The Material in the Management Directive documents (Management Directive #0460.1 Freedom of Information Act Compliance and Management Directive #11042, Safeguarding Sensitive but Unclassified (SBU) Information) have been superseded by newer versions but have been included because of their historical significance.

Department of Homeland Security

Administrative Record Support

MD 5100.1, Environmental Planning Program

About the Center for Domestic Preparedness (CDP)

Mission Statement To operate a federal training center specializing in providing advanced and hands-on training to America's federal, state, local, tribal, and parish emergency responders, to prevent, deter, respond to, and recover from terrorist acts, especially those involving weapons of mass destruction or hazardous materials.

Message from the Director F. Marion Cain III

History Events over the past few years have shown that terrorist, foreign and domestic, are willing to attack American interests at home and abroad. Terrorists now have access to a broad array of advanced technologies and lethal materials worldwide. International and domestic terrorism can strike any target at any time, and terrorists are no longer limited to conventional weapons. There is concern that chemical and biological agents are weapons of choice.

On June 1, 1998, the Center for Domestic Preparedness was officially established under the Department of Justice as a Training Center for Emergency Responders to terrorist acts. Under the Homeland Security Act of 2002, the Center became part of the newly created Department of Homeland Security.

Since the Center opened and began training operations on June 1, 1998, emergency responders have received invaluable training which will assist them in dealing with a terrorist attack. They gain critical skills and necessary confidence which enables them to effectively respond to a Weapons of Mass Destruction incident.

The Center for Domestic Preparedness, US Department of Homeland Security, is charged with training emergency responders: law enforcement, firefighters, emergency medical personnel and others to deal with a terrorist attack involving Weapons of Mass Destruction and incidents involving hazardous materials. An awesome task when you realize there are more than 11 million emergency responders and other personnel in this country that would need training to deal with terrorist incidents.

Department of Homeland Security

Administrative Record Support

MD 5100.1, Environmental Planning Program

Definition of Bioengineering

Bioengineering is the use of either native or proven vegetative species to put down roots and stabilize the soil along a water course. Branches, whips, cuttings, rooted cuttings, and stakes are examples of what may be used. Species such as willows, dogwoods, and poplars are used. Such materials can be collected locally or purchased from suppliers recommended by the local office of the Untied States Department of Agriculture (USDA) Natural Resources Conservation Service (NRCS). The use of such techniques is relatively inexpensive and highly preferable to mitigating the results of siltation caused by soil disturbing activities.

Department of Homeland Security
Management Directive System
MD Number: 11042

Issue Date: 5/11/2004

SAFEGUARDING SENSITIVE BUT UNCLASSIFIED (FOR OFFICIAL USE ONLY) INFORMATION

1. Purpose

This directive establishes Department of Homeland Security (DHS) policy regarding the identification and safeguarding of sensitive but unclassified information originated within DHS. It also applies to other sensitive but unclassified information received by DHS from other government and non-governmental activities.

2. Scope

This directive is applicable to all DHS Headquarters, components, organizational elements, contractors, consultants, and others to whom access to information covered by this directive is granted.

3. Authorities

Homeland Security Act of 2002.

4. Definitions

Access: The ability or opportunity to gain knowledge of information.

For Official Use Only (FOUO): The term used within DHS to identify unclassified information of a sensitive nature, not otherwise categorized by statute or regulation, the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national interest. Information impacting the National Security of the United States and classified Confidential, Secret, or Top Secret under Executive Order 12958, "Classified National Security Information," as amended, or its predecessor or successor orders, is not to be considered FOUO. FOUO is not to be considered classified information.

Need-to-know: The determination made by an authorized holder of information that a prospective recipient requires access to specific information in order to

perform or assist in a lawful and authorized governmental function, i.e., access is required for the performance of official duties.

Organizational Element: As used in this directive, organizational element is as defined in DHS MD Number 0010.1, Management Directive System and DHS Announcements.

Protected Critical Infrastructure Information (PCII): Critical infrastructure information (CII) is defined in 6 U.S.C. 131(3) (Section 212(3) of the Homeland Security Act). Critical infrastructure information means information not customarily in the public domain and related to the security of critical infrastructure or protected systems. Protected Critical Infrastructure Information is a subset of CII that is voluntarily submitted to the Federal Government and for which protection is requested under the PCII program by the requestor.

Sensitive Security Information (SSI): Sensitive security information (SSI) is defined in 49 C.F.R. Part 1520. SSI is a specific category of information that requires protection against disclosure. 49 U.S.C. 40119 limits the disclosure of information obtained or developed in carrying out certain security or research and development activities to the extent that it has been determined that disclosure of the information would be an unwarranted invasion of personal privacy; reveal a trade secret or privileged or confidential commercial or financial information; or be detrimental to the safety of passengers in transportation.

5. Responsibilities

A. The DHS Office of Security will:

1. Be responsible for practical application of all aspects of the program to protect FOUO.

2. Promulgate Department-wide policy guidance.

B. Heads of DHS Organizational Elements will:

1. Ensure compliance with the standards for safeguarding sensitive but unclassified information as cited in this directive.

2. Designate an official to serve as a Security Officer or Security Liaison.

C. The organizational element's Security Officer/Security Liaison will:

Be responsible for implementation and oversight of the FOUO information protection program and will serve as liaison between the DHS Office of Security and other organizational security officers.

D. DHS employees, contractors, consultants and others to whom access is granted will:

1. Be aware of and comply with the safeguarding requirements for FOUO information as outlined in this directive.

2. Be aware that divulging information without proper authority could result in administrative or disciplinary action.

3. Execute a DHS Form 11000-6, Sensitive But Unclassified Information Non-Disclosure Agreement (NdA), upon initial assignment to DHS. Other individuals not assigned to or contractually obligated to DHS, but to whom access to information will be granted, may be requested to execute an NdA as determined by the program manager to which they will have access.

E. Supervisors and managers will:

1. Ensure that an adequate level of education and awareness is established and maintained that serves to emphasize safeguarding and prevent unauthorized disclosure of FOUO information.

2. Take appropriate corrective actions, to include administrative or disciplinary action as appropriate, when violations occur.

6. Policy and Procedures

A. General

1. The Computer Security Act of 1987, Public Law 100-235, defines "sensitive information" as "any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, United States Code (the Privacy Act) but which has not been specifically authorized under criteria established by an executive order or an act of Congress to be kept secret in the interest of national defense or foreign policy." However, with the exception of certain types of information protected by statute, specific, standard criteria and terminology defining the types of information warranting designation as "sensitive information" does not exist within the Federal government. Such designations are left to the discretion of each individual agency.

2. Within the "sensitive but unclassified" arena, in addition to the various categories of information specifically described and protected by statute or regulation, e.g., Tax Return Information, Privacy Act Information, Sensitive Security Information (SSI), Critical Infrastructure Information (CII), Grand Jury

Information, etc. There are numerous additional caveats used by various agencies to identify unclassified information as sensitive, e.g., For Official Use Only; Law Enforcement Sensitive; Official Use Only; Limited Official Use; etc. Regardless of the caveat used to identify it, however, the reason for the designation does not change. Information is designated as sensitive to control and restrict access to certain information, the release of which could cause harm to a person's privacy or welfare, adversely impact economic or industrial institutions, or compromise programs or operations essential to the safeguarding of our national interests.

3. Designation of information as FOUO is not a vehicle for concealing government negligence, ineptitude, illegalities, or other disreputable circumstances embarrassing to a government agency.

4. Information designated as FOUO is not automatically exempt from disclosure under the provisions of the Freedom of Information Act, 5 U.S.C. 552, (FOIA). Information requested by the public under a FOIA request must still be reviewed on a case-by-case basis.

B. For Official Use Only

Within DHS, the caveat "FOR OFFICIAL USE ONLY" will be used to identify sensitive but unclassified information within the DHS community that is not otherwise specifically described and governed by statute or regulation. The use of these and other approved caveats will be governed by the statutes and regulations issued for the applicable category of information.

C. Information Designated as FOUO

1. The following types of information will be treated as FOUO information. Where information cited below also meets the standards for designation pursuant to other existing statutes or regulations, the applicable statutory or regulatory guidance will take precedence. For example, should information meet the standards for designation as Sensitive Security Information (SSI), then SSI guidance for marking, handling, and safeguarding will take precedence.

(a) Information of the type that may be exempt from disclosure per 5 U.S.C. 552, Freedom of Information Act, and its amendments. Designation of information as FOUO does not imply that the information is already exempt from disclosure under FOIA. Requests under FOIA, for information designated as FOUO, will be reviewed and processed in the same manner as any other FOIA request.

(b) Information exempt from disclosure per 5 U.S.C. 552a, Privacy Act.

(c) Information within the international and domestic banking and financial communities protected by statute, treaty, or other agreements.

(d) Other international and domestic information protected by statute, treaty, regulation or other agreements.

(e) Information that could be sold for profit.

(f) Information that could result in physical risk to personnel.

(g) DHS information technology (IT) internal systems data revealing infrastructure used for servers, desktops, and networks; applications name, version and release; switching, router, and gateway information; interconnections and access methods; mission or business use/need. Examples of information are systems inventories and enterprise architecture models. Information pertaining to national security systems and eligible for classification under Executive Order 12958, as amended, will be classified as appropriate.

(h) Systems security data revealing the security posture of the system. For example, threat assessments, system security plans, contingency plans, risk management plans, Business Impact Analysis studies, and Certification and Accreditation documentation.

(i) Reviews or reports illustrating or disclosing facility infrastructure or security vulnerabilities, whether to persons, systems, or facilities, not otherwise eligible for classification under Executive Order 12958, as amended.

(j) Information that could constitute an indicator of U.S. government intentions, capabilities, operations, or activities or otherwise threaten operations security.

(k) Developing or current technology, the release of which could hinder the objectives of DHS, compromise a technological advantage or countermeasure, cause a denial of service, or provide an adversary with sufficient information to clone, counterfeit, or circumvent a process or system.

2. Other government agencies and international organizations may use different terminology to identify sensitive information, such as “Limited Official Use (LOU),” and “Official Use Only (OUO).” In most instances the safeguarding requirements for this type of information are equivalent to FOUO. However, other agencies and international organizations may have additional requirements concerning the safeguarding of sensitive information. Follow the safeguarding guidance provided by the other agency or organization. Should there be no such

guidance, the information will be safeguarded in accordance with the requirements for FOUO as provided in this manual. Should the additional guidance be less restrictive than in this directive, the information will be safeguarded in accordance with this directive.

D. Designation Authority

Any DHS employee, detailee, or contractor can designate information falling within one or more of the categories cited in section 6, paragraph C, as FOUO. Officials occupying supervisory or managerial positions are authorized to designate other information, not listed above and originating under their jurisdiction, as FOUO.

E. Duration of Designation

Information designated as FOUO will retain its designation until determined otherwise by the originator or a supervisory or management official having program management responsibility over the originator and/or the information.

F. Marking

1. Information designated as FOUO will be sufficiently marked so that persons having access to it are aware of its sensitivity and protection requirements. The lack of FOUO markings on materials does not relieve the holder from safeguarding responsibilities. Where the FOUO marking is not present on materials known by the holder to be FOUO, the holder of the material will protect it as FOUO. Other sensitive information protected by statute or regulation, e.g., PCII and SSI, etc., will be marked in accordance with the applicable guidance for that type of information. Information marked in accordance with the guidance provided for the type of information need not be additionally marked FOUO.

(a) Prominently mark the bottom of the front cover, first page, title page, back cover and each individual page containing FOUO information with the caveat “FOR OFFICIAL USE ONLY.”

(b) Materials containing specific types of FOUO may be further marked with the applicable caveat, e.g., “LAW ENFORCEMENT SENSITIVE,” in order to alert the reader of the type of information conveyed. Where the sensitivity of the information warrants additional access and dissemination restrictions, the originator may cite additional access and dissemination restrictions. For example:

WARNING: *This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This*

information shall not be distributed beyond the original addressees without prior authorization of the originator.

(c) Materials being transmitted to recipients outside of DHS, for example, other federal agencies, state or local officials, etc. who may not be aware of what the FOUO caveat represents, shall include the following additional notice:

WARNING: *This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.*

(d) Computer storage media, i.e., disks, tapes, removable drives, etc., containing FOUO information will be marked "FOR OFFICIAL USE ONLY."

(e) Portions of a classified document, i.e., subjects, titles, paragraphs, and subparagraphs that contain only FOUO information will be marked with the abbreviation (FOUO).

(f) Individual portion markings on a document that contains no other designation are not required.

(g) Designator or originator information and markings, downgrading instructions, and date/event markings are not required.

G. General Handling Procedures

Although FOUO is the DHS standard caveat for identifying sensitive unclassified information, some types of FOUO information may be more sensitive than others and thus warrant additional safeguarding measures beyond the minimum requirements established in this manual. For example, certain types of information may be considered extremely sensitive based on the repercussions that could result should the information be released or compromised. Such repercussions could be the loss of life or compromise of an informant or operation. Additional control requirements may be added as necessary to afford appropriate protection to the information. DHS employees, contractors, and detailees must use sound judgment coupled with an evaluation of the risks, vulnerabilities, and the potential damage to personnel or property as the basis for determining the need for safeguards in excess of the minimum requirements and protect the information accordingly.

1. When removed from an authorized storage location (see section 6.I) and persons without a need-to-know are present, or where casual observation would reveal FOUO information to unauthorized persons, a “FOR OFFICIAL USE ONLY” cover sheet (Enclosure 1) will be used to prevent unauthorized or inadvertent disclosure.

2. When forwarding FOUO information, a FOUO cover sheet should be placed on top of the transmittal letter, memorandum or document.

3. When receiving FOUO equivalent information from another government agency, handle in accordance with the guidance provided by the other government agency. Where no guidance is provided, handle in accordance with the requirements of this directive.

H. Dissemination and Access

1. FOUO information will not be disseminated in any manner - orally, visually, or electronically - to unauthorized personnel.

2. Access to FOUO information is based on “need-to-know” as determined by the holder of the information. Where there is uncertainty as to a person’s need-to-know, the holder of the information will request dissemination instructions from their next-level supervisor or the information’s originator.

3. The holder of the information will comply with any access and dissemination restrictions.

4. A security clearance is not required for access to FOUO information.

5. When discussing or transferring FOUO information to another individual(s), ensure that the individual with whom the discussion is to be held or the information is to be transferred has a valid need-to-know, and that precautions are taken to prevent unauthorized individuals from overhearing the conversation, observing the materials, or otherwise obtaining the information.

6. FOUO information may be shared with other agencies, federal, state, tribal, or local government and law enforcement officials, provided a specific need-to-know has been established and the information is shared in furtherance of a coordinated and official governmental activity. Where FOUO information is requested by an official of another agency and there is no coordinated or other official governmental activity, a written request will be made from the requesting agency to the applicable DHS program office providing the name(s) of personnel for whom access is requested, the specific information to which access is requested, and basis for need-to-know. The DHS program office shall then determine if it is appropriate to release the information to the other agency official. (see section 6.F for marking requirements)

7. Other sensitive information protected by statute or regulation, i.e., Privacy Act, CII, SSI, Grand Jury, etc., will be controlled and disseminated in accordance with the applicable guidance for that type of information.

8. If the information requested or to be discussed belongs to another agency or organization, comply with that agency's policy concerning third party discussion and dissemination.

9. When discussing FOUO information over a telephone, the use of a STU III (Secure Telephone Unit), or Secure Telephone Equipment (STE), is encouraged, but not required.

I. Storage

1. When unattended, FOUO materials will, at a minimum, be stored in a locked file cabinet, locked desk drawer, a locked overhead storage compartment such as a systems furniture credenza, or similar locked compartment. Materials can also be stored in a room or area that has sufficient physical access control measures to afford adequate protection and prevent unauthorized access by members of the public, visitors, or other persons without a need-to-know, such as a locked room, or an area where access is controlled by a guard, cipher lock, or card reader.

2. FOUO information will not be stored in the same container used for the storage of classified information unless there is a correlation between the information. When FOUO materials are stored in the same container used for the storage of classified materials, they will be segregated from the classified materials to the extent possible, i.e. separate folders, separate drawers, etc.

3. IT systems that store FOUO information will be certified and accredited for operation in accordance with federal and DHS standards. Consult the DHS Information Technology Security Program Handbook for Sensitive Systems, Publication 4300A, for more detailed information.

4. Laptop computers and other media containing FOUO information will be stored and protected to prevent loss, theft, unauthorized access and unauthorized disclosure. Storage and control will be in accordance with DHS Information Technology Security Program Handbook for Sensitive Systems, Publication 4300A.

J. Transmission

1. Transmission of hard copy FOUO within the U.S. and its Territories:

(a) Material will be placed in a single opaque envelope or container and sufficiently sealed to prevent inadvertent opening and to show evidence of tampering. The envelope or container will bear the complete name and address of the sender and addressee, to include program office and the name of the intended recipient (if known).

(b) FOUO materials may be mailed by U.S. Postal Service First Class Mail or an accountable commercial delivery service such as Federal Express or United Parcel Service.

(c) FOUO materials may be entered into an inter-office mail system provided it is afforded sufficient protection to prevent unauthorized access, e.g., sealed envelope.

2. Transmission to Overseas Offices: When an overseas office is serviced by a military postal facility, i.e., APO/FPO, FOUO may be transmitted directly to the office. Where the overseas office is not serviced by a military postal facility, the materials will be sent through the Department of State, Diplomatic Courier.

3. Electronic Transmission.

(a) Transmittal via Fax. Unless otherwise restricted by the originator, FOUO information may be sent via nonsecure fax. However, the use of a secure fax machine is highly encouraged. Where a nonsecure fax is used, the sender will coordinate with the recipient to ensure that the materials faxed will not be left unattended or subjected to possible unauthorized disclosure on the receiving end. The holder of the material will comply with any access, dissemination, and transmittal restrictions cited on the material or verbally communicated by the originator.

(b) Transmittal via E-Mail

(i) FOUO information transmitted via email should be protected by encryption or transmitted within secure communications systems. When this is impractical or unavailable, FOUO may be transmitted over regular email channels. For added security, when transmitting FOUO over a regular email channel, the information can be included as a password protected attachment with the password provided under separate cover. Recipients of FOUO information will comply with any email restrictions imposed by the originator.

(ii) Per DHS MD 4300, DHS Sensitive Systems Handbook, due to inherent vulnerabilities, FOUO information shall not be sent to personal email accounts.

(c) DHS Internet/Intranet

(i) FOUO information will not be posted on a DHS or any other internet (public) website.

(ii) FOUO information may be posted on the DHS intranet or other government controlled or sponsored protected encrypted data networks, such as the Homeland Security Information Network (HSIN). However, the official authorized to post the information should be aware that access to the information is open to all personnel who have been granted access to that particular intranet site. The official must determine the nature of the information is such that need-to-know applies to all personnel; the benefits of posting the information outweigh the risk of potential compromise; the information posted is prominently marked as FOR OFFICIAL USE ONLY; and information posted does not violate any provisions of the Privacy Act.

K. Destruction

1. FOUO material will be destroyed when no longer needed. Destruction may be accomplished by:

(a) "Hard Copy" materials will be destroyed by shredding, burning, pulping, pulverizing, such as to assure destruction beyond recognition and reconstruction. After destruction, materials may be disposed of with normal waste.

(b) Electronic storage media shall be sanitized appropriately by overwriting or degaussing. Contact local IT security personnel for additional guidance.

(c) Paper products containing FOUO information will not be disposed of in regular trash or recycling receptacles unless the materials have first been destroyed as specified above.

L. Incident Reporting

1. The loss, compromise, suspected compromise, or unauthorized disclosure of FOUO information will be reported. Incidents involving FOUO in DHS IT systems will be reported to the organizational element Computer Security Incident Response Center in accordance with IT incident reporting requirements.

2. Suspicious or inappropriate requests for information by any means, e.g., email or verbal, shall be report to the DHS Office of Security.

3. Employees or contractors who observe or become aware of the loss, compromise, suspected compromise, or unauthorized disclosure of FOUO information will report it immediately, but not later than the next duty day, to the originator and the local Security Official.

4. Additional notifications to appropriate DHS management personnel will be made without delay when the disclosure or compromise could result in physical harm to an individual(s) or the compromise of a planned or on-going operation.

5. At the request of the originator, an inquiry will be conducted by the local security official or other designee to determine the cause and affect of the incident and the appropriateness of administrative or disciplinary action against the offender.

Department of Homeland Security

FOR OFFICIAL USE ONLY

THE ATTACHED MATERIALS CONTAIN DEPARTMENT OF HOMELAND SECURITY INFORMATION THAT IS "FOR OFFICIAL USE ONLY," OR OTHER TYPES OF SENSITIVE BUT UNCLASSIFIED INFORMATION REQUIRING PROTECTION AGAINST UNAUTHORIZED DISCLOSURE. THE ATTACHED MATERIALS WILL BE HANDLED AND SAFEGUARDED IN ACCORDANCE WITH DHS MANAGEMENT DIRECTIVES GOVERNING PROTECTION AND DISSEMINATION OF SUCH INFORMATION.

AT A MINIMUM, THE ATTACHED MATERIALS WILL BE DISSEMINATED ONLY ON A "NEED-TO-KNOW" BASIS AND WHEN UNATTENDED, WILL BE STORED IN A LOCKED CONTAINER OR AREA OFFERING SUFFICIENT PROTECTION AGAINST THEFT, COMPROMISE, INADVERTENT ACCESS AND UNAUTHORIZED DISCLOSURE.

FREEDOM OF INFORMATION ACT COMPLIANCE

1. Purpose

This directive establishes the Department of Homeland Security (DHS) policy for the Freedom of Information Act (FOIA), as amended.

2. Scope

This directive applies to all DHS organizational elements.

3. Authorities

This directive is governed by numerous Executive Orders, Public Laws, and national policy, such as:

A. The Freedom of Information Act, as amended (5 U.S.C. 552).

B. Paperwork Reduction Act of 1995, Pub. L. No. 104-13. Department of Justice Fee Waiver Policy Guidance, dated April 2, 1987.

C. E.O. 12600, "Predisclosure Notification Procedures for Confidential Commercial Information", dated June 23, 1987.

D. E.O. 12958, "National Security Information."

E. Freedom of Information Reform Act of 1986; Uniform Freedom of Information Act Fee Schedule and Guidelines; 52 Federal Register 10012, dated March 27, 1987.

F. President's Memorandum For Heads of Departments and Agencies, dated October 4, 1993, subject: The Freedom of Information Act.

G. Attorney General's Memorandum on the 1986 Amendments to the Freedom of Information Act;

H. Attorney General's Memorandum for Heads of All Federal Departments and Agencies Regarding the FOIA, October 12, 2001

I. Guidance on Homeland Security Information, March 19, 2002

4. Definitions

A. **Category:** The classification assigned to a requester for fee purposes determined by the projected use of the records. The categories are: (a) commercial; (b) educational; (c) non-commercial scientific institutions; (d) representative of the news media; and (e) all other requesters.

B. **Department:** The Department of Homeland Security (DHS).

C. **FOIA Officer:** FOIA Officer refers to an employee selected by an Under Secretary or a Designated DHS official to receive FOIA requests assigned to their area by the Departmental Disclosure Officer and to provide assistance in administrative matters pertaining to FOIA request processing. For other offices, FOIA Officer refers to the head of each disclosure office.

D. **Responsible Official:** The head of the organizational unit having immediate custody of the records requested or a designated official. The responsible official makes initial determinations to grant or deny requests for access to records and requests for fee waivers. The responsible official will also determine a requester's category for fee purposes.

E. **Designated DHS Official**: Senior DHS officials as designated by the Secretary, Deputy Secretary or Under Secretaries.

F. **Departmental Disclosure Officer (DDO)**: An individual reporting to the Under Secretary for Management who serves as the Department of the Homeland Security's principal point of contact and agency representative on FOIA-related matters.

G. **Appeal Authority:** The Assistant General Counsel for General Law or his or her designee.

5. Responsibilities

A. **All Under Secretaries and Designated DHS Officials:** shall be responsible for the following tasks relating to their area of responsibility:

1. establish internal procedures to ensure the effectiveness of the Department's FOIA program. For organizational elements transferring into DHS where such internal procedures may already exist, they may continue to be used until amended or replaced by the DHS DDO. Any new procedures shall be consistent with this

directive and: (a)
the FOIA, as amended; (b)
Executive Order (E.O.) 12600; (c)
E.O. 12958; and, (d)
applicable Department of Justice, Office of Management and Budget, and National Archives and Records Administration guidelines.

2. ensure that employees who are responsible in any part for FOIA processing are knowledgeable about the provisions and requirements of the FOIA and ensure that these employees attend FOIA training at least once a year;

3. ensure that accurate and complete data is submitted in a timely manner to the Departmental Disclosure Officer for the Department of Homeland Security's Annual FOIA Report to the Attorney General, and for other reporting purposes, as required;

4. ensure that records that are subject to section (a)(2) of the FOIA which have been created on or after November 1, 1996, are posted;

5. submit proposed organizational element disclosure regulations or proposed changes to regulations to the Departmental Disclosure Officer for review;

6. select a FOIA Officer and advise the Departmental Disclosure Officer of the selection and of any subsequent changes in designation of selection;

7. ensure that directorate FOIA Officers and web masters collaborate with directorate records management officers prior to disposing of records posted on the FOIA web sites and to schedule electronic records on the sites; and

8. ensure that reasonable efforts are made to maintain records in forms or formats that are reproducible for purposes of the FOIA.

B. The **Under Secretary for Management** shall:

1. provide technical management support for the Department's FOIA web site on the DHS Internet and technical assistance to the Departmental Disclosure Officer to ensure compliance with the requirements of the FOIA;

2. provide technical assistance to directorates in placing records in the electronic reading room which includes establishing specific procedures for maintaining and posting directorate records;

3. establish and maintain an index of all major information systems and a description of major information and record locator systems in the Department;

4. ensure that DHS-wide, cost-effective, state-of-the-art technical solutions for electronic redaction are implemented to achieve economies of scale and integrate with the information technology infrastructure;

5. provide information technology guidance to DHS FOIA Officers, web masters, and records management officers regarding information posted on the DHS FOIA web sites; and

6. provide oversight, guidance and support to the Departmental Disclosure Officer.

C. The **Departmental Disclosure Officer (DDO)** shall:

1. act as the Department of the Homeland Security's principal point of contact and agency representative on FOIA-related matters;

2. coordinate the Department's FOIA implementation and management in collaboration with DHS organizational elements;

3. provide regulatory and policy guidance, and technical advice and assistance to the Department on FOIA-related matters;

4. review proposed changes to DHS disclosure regulations;

5. collect, review, consolidate, and submit the data for the Annual FOIA Report to the Attorney General on behalf of the Department;

6. post Departmental Office (DO) records that are subject to section (a)(2) of the FOIA which have been created on or after November 1, 1996;

7. grant or deny requests for expedited processing of requests for DO records;

8. supervise the implementation of the FOIA within the DO;

9. notify a requester when information needed to process a request for DO records is lacking;

10. assign FOIA requests to the appropriate FOIA Officer for action;

11. assign FOIA appeals to the appropriate appeal authority within DO;

12. follow up with the assigned office to ensure completion of a request or appeal, when necessary;

13. when a request seeks records in the custody of two or more functions within DO for which separate FOIA Officers have been designated, assign to one of the FOIA Officers the responsibility of coordinating one response;

14. assist the general public in making FOIA requests to the Department; and

15. conduct FOIA training on a regular basis and oversee the FOIA training conducted at DHS offices.

D. **Responsible Officials** shall:

1. determine:

(a) whether to grant or deny requests for access to records;
(b) whether to grant or deny requests for fee waivers; and,
(c) a requester's category for fee purposes;

2. notify the requester of determination(s) made pursuant to paragraph 5.D.1;

3. determine costs incurred by the Department to process the request and whether or not fees will be charged to the requester;

4. ensure that requests are processed in accordance with all applicable disclosure requirements;

5. compile and provide data for the Annual FOIA Report; and,

6. retrieve records retired to the Federal Records Center if they are needed in processing a request.

E. **Appeal Authority** shall, upon receipt of an administrative appeal, either affirm or reverse those initial determinations that:

1. deny access to a record or portion thereof;

2. deny a request for a fee waiver;

3. pertain to a requester's category;

4. advise of no records located; or

5. deny a request for expedited processing.

F. **FOIA Officers** shall:

1. designate a responsible official to respond to each FOIA request received or assigned pursuant to paragraph 5.C.10;

2. ensure consistency and completeness of a Departmental response when assigned responsibility for coordination pursuant to paragraph 5.C.13;

3. determine, with appropriate program officials, which records in response to FOIA requests have become or are likely to become the subject of repeated requests for the same records and ensure that these records are placed in the electronic reading room of the Department's web site; and,

4. coordinate with the Department web masters and records management officers regarding the disposing of records in the electronic reading room of the Department's web site.

6. Policy & Procedures

A. **Policy:** It is the policy of DHS to implement the FOIA uniformly and consistently and to provide maximum allowable disclosure of agency records upon request by any individual.

B. **Procedures:** Upon receipt of a request satisfying the requirements of the FOIA, records shall be disclosed unless they are protected by one or more of the FOIA exemptions or exclusions and are not appropriate for discretionary disclosure. Requests shall be processed within the time limits defined by the FOIA. Individuals requesting information will be informed of the right and procedure to seek administrative appeal and to seek judicial review of:

1. any partial or total denial of access to records;
2. a fee waiver denial;
3. a determination of requester's category for fee purposes;
4. a no-records determination; or,
5. a denial of a request for expedited processing.

The FOIA requires that, except in "unusual circumstances" as specified in the Act, agency initial decisions on whether to grant or deny access to records must be made within 20 working days of receiving the request and the requester so notified. A requester may administratively appeal an agency's adverse initial determination and may seek judicial review if not satisfied with the agency's final decision. If a court determines that agency personnel have acted arbitrarily or capriciously in withholding records, disciplinary action against the employee primarily responsible may be warranted.

C. **Questions or Concerns Regarding the Process:** Any questions or concerns regarding this directive should be addressed to the DDO.

U.S. Department of Homeland Security
Arlington, Virginia 22202-4220

Transportation Security Administration

May 13, 2004

MEMORANDUM FOR David Reese
Senior Environmental Specialist
Department of Homeland Security

THROUGH: Thomas Muther
Attorney Advisor
Department of Homeland Security

FROM: Elizabeth F. Buchanan
Assistant Chief Counsel for
Ethics and General Legal Services

SUBJECT: Administrative Record for Transportation Security Administration (TSA) Categorical Exclusions

SUMMARY

TSA requested a list of categorical exclusions to be adopted as part of the Department of Homeland Security (DHS) regulations implementing the National Environmental Policy Act (NEPA).[1] We have since agreed with DHS that our proposed categorical exclusions numbers H1, H5, H6, and H8 are encompassed within other proposed categorical exclusions that apply DHS-wide. Therefore, we agreed to drop our request with regard to those proposals. The Council for Environmental Quality (CEQ) has asked for an administrative record to support the balance of the proposals.

1

CATEGORICAL EXCLUSIONS FOR THE TRANSPORTATION AND SECURITY ADMINISTRATION
H1 Installation or removal of equipment to screen passengers, baggage, or cargo at existing facilities.
H2 Issuance of grants for the conduct of security-related research and development or the implementation of security plans or other measures at existing facilities.
H3 Issuance of planning documents and advisory circulars on planning for security measures which are not intended for direct implementation or are issued as administrative and technical guidance.
H4 Issuance or revocation of certificates or other approvals, including but not limited to: (a) Airmen certificates (b) Security procedures at general aviation airports (c) Airport security plans
H5 Emergency measures regarding air or ground security.
H6 Training and exercises in planning or adopting security measures or in emergency preparedness.
H7 Approval or disapproval of security plans required under legislative or regulatory mandates unless such plans would have a significant effect on the environment.
H8 Construction that does not significantly alter land use including minor construction within airport facilities to accommodate installation, removal, and operation of security equipment.

All of TSA's proposals are based on existing approved FAA categorical exclusions. TSA uses FAA's categorical exclusions until the DHS NEPA implementing regulation is approved because of the savings clause in the act that created TSA. TSA was created in the Aviation and Transportation Security Act (ATSA), Pub.L. 107-71. As part of that Act, the civil aviation security function was transferred from FAA to TSA. ATSA, section 101(g). ATSA further contains a savings clause, which provided that all "orders, determinations, rules, regulations, permits, grants, loans, contracts, settlements, agreements, certificates, licenses, and privileges – (1) that have been issued, made, granted, or allowed to become effective by the Federal Aviation Administration, any officer or employee thereof, or any other Government official, or by a court of competent jurisdiction, in the performance of any function that is transferred by this Act; and (2) that are in effect on the effective date of such transfer (or become effective after such date pursuant to their terms as in effect on such effective date), shall continue in effect according to their terms until modified, terminated, superseded, set aside, or revoked in accordance with law by the Under Secretary of Transportation for Security[2], any other authorized official, a court of competent jurisdiction, or operation of law." ATSA, section 141(b). As a result of this savings clause, all of the regulations of the FAA that were in effect on the date of ATSA (November 19, 2001) continue to apply to TSA, including FAA's NEPA implementation.

TSA was transferred to DHS as a result of the Homeland Security Act of 2002 (HSA), Pub.L. 107-276. HSA, section 403. The HSA also contained a savings clause, which provides that all completed administrative actions of an agency shall not be affected by the enactment of this Act or by the transfer of such agency to the Department but shall continue in effect according to their terms until amended, modified, superseded, set aside, or revoked in accordance with law by an officer of the United States or a court of competent jurisdiction, or by operation of law. HSA, section 1512(a)(1). "Completed administrative actions" for purposes of this section includes orders, determinations, rules, regulations, personnel actions, permits, agreements, grants, contracts, certificates, licenses, registrations, and privileges. HSA, section 1512(a)(2). As a result of this savings clause, all of the regulations that had applied to TSA on the date of transfer to DHS, including all effective regulations of FAA, continue to apply until superseded.

FAA's regulations for implementing NEPA are found in FAA Order 1050.1D, Policies and Procedures for Considering Environmental Impacts. See 64 Fed. Reg. 55526 for a description of the existing order plus proposed changes. TSA tailored FAA categorical exemptions that it uses to ensure that they were as narrowly written as possible. The specific categorical exclusions (Cat Ex) upon which TSA relies for its proposals H2, H3, H4, and H7 are:

1. H2: Issuance of grants for the conduct of security-related research and development or the implementation of security plans or other measures at existing facilities.

[2] ATSA created TSA as an agency within the Department of Transportation and referred to the head of TSA as the Under Secretary of Transportation for Security. Since the transfer of TSA to the Department of Homeland Security pursuant to the Homeland Security Act of 2002, Pub. L. 1078-296, 116 Stat. 2135 (November 25, 2002), the title of the head of TSA has been administratively changed to "Administrator."

FAA Cat Ex: FAA Order 1050.1D, appendix 3, para 4.g.: Procedural actions requested by users on a test basis to determine the effectiveness of new technology and measurement of possible impacts on the environment.

FAA Cat Ex: Proposed FAA Order 1050.1E, Figure 3-2, Existing Equipment and Implementation Action 5[3]: Federal financial assistance or Airport Layout Plan (ALP) approval of miscellaneous items including wind indicators, wind measuring devices, landing directional equipment, segmented circles (visual indicators providing traffic pattern information at airports without air traffic control towers) and fencing.

FAA Cat Ex: Proposed FAA Order 1050.1E, Figure 3-2, Existing Equipment and Implementation Action 9[4]: Acquisition of security equipment required by rule or regulation for the safety and security of personnel and property on the airport (14 CFR Part 107, Airport Security), safety equipment required by rule or regulation for certification of an airport (14 CFR part 139, Certification and Operation: Land Airports Serving Certain Air Carriers) or snow removal equipment.

2. H3: Issuance of planning documents and advisory circulars on planning for security measures which are not intended for direct implementation or are issued as administrative and technical guidance.

FAA Cat Ex: FAA Order 1050.1D, chapter 3.a.(5): Policy and planning documents not intended for or which do not cause direct implementation of project or system actions.

FAA Cat Ex: FAA Order 1050.1D, appendix 3, para 4.d.: Actions taken under … FAR Part 99, "Security Control of Air Traffic."

FAA Cat Ex: Proposed FAA Order 1050.1E, Figure 3-2, Existing Administrative/General Action 7[5]: Issuance of airport policy and planning documents including the National Plan of Integrated Airport Systems (NPIAS), Airport Improvement Program (AIP) priority system, and advisory circulars on planning, design, and development which are issued as administrative and technical guidance.

3. H4: Issuance or revocation of certificates or other approvals, including but not limited to:

(a) Airmen certificates
(b) Security procedures at general aviation airports
(c) Airport security plans

FAA Cat Ex: FAA Order 1050.1D, chapter 3.a.(8): The approval or issuance of certificates covering medicals for airmen, delegated authority, ground

[3] Please note that where we have cited the proposed draft FAA Order 1050.1E, we are only using categorical exclusions that are noted as being already approved and in existence.
[4] Please note that where we have cited the proposed draft FAA Order 1050.1E, we are only using categorical exclusions that are noted as being already approved and in existence.
[5] Please note that where we have cited the proposed draft FAA Order 1050.1E, we are only using categorical exclusions that are noted as being already approved and in existence.

schools, out-of-agency training and aircraft repair or maintenance not affecting noise, emissions, or wastes.

FAA Cat Ex: FAA Order 1050.1D, Appendix 4, para 4.a.: Certificates for new, amended, or supplemental … (4) medical, airmen, export, manned free balloon type, glider type, propeller type, supplemental type not affecting noise, emission or waste; and (5) mechanic schools, agricultural aircraft operations, repair stations and other air agency ratings.

FAA Cat Ex: Proposed FAA Order 1050.1E, Figure 3-2, Existing Administrative/General Action 7[6]: Issuance of airport policy and planning documents including the National Plan of Integrated Airport Systems (NPIAS), Airport Improvement Program (AIP) priority system, and advisory circulars on planning, design, and development which are issued as administrative and technical guidance.

FAA Cat Ex: FAA Order 1050.1D, appendix 3, para 4.d.: Actions taken under … FAR Part 99, "Security Control of Air Traffic."

4. H7: Approval or disapproval of security plans required under legislative or regulatory mandates unless such plans would have a significant effect on the environment.

FAA Cat Ex: FAA Order 1050.1D, Appendix 4, para 4.k.: Regulations, standards, and exemptions (excluding those which if implemented may cause a significant impact on the human environment).

FAA Cat Ex: FAA Order 1050.1D, appendix 3, para 4.d.: Actions taken under … FAR Part 99, "Security Control of Air Traffic."

[6] Please note that where we have cited the proposed draft FAA Order 1050.1E, we are only using categorical exclusions that are noted as being already approved and in existence.

Department of Homeland Security

Administrative Record Support

MD 5100.1, Environmental Planning Program

Members of the Panel of Environmental Professionals

Paul Atelsek

Attorney-Advisor. Headquarters, United States Coast Guard (Office of The Judge Advocate General). 14 years experience. Master of Science in Geology, Juris Doctor

Alfred Crescenzi

Industrial Hygienist, Environmental Measurements Laboratory (EML) Science and Technology Directorate (S&T). Length of time employed in your current operational element: Employed 21 years in the Environmental &Occupational Safety & Health Profession with 15 years at EML. 20 years experience with federal facilities environmental compliance issues and six years experience in the private sector. Master of Science in Environmental Health Science

Francis H. Esposito

Environmental Planning Attorney. Headquarters, United States Coast Guard (Office of The Judge Advocate General). 27 years, with 6 years at Coast Guard. BS Cornel University Col of Civil and Environmental Engineering, JD University of Ky Col of Law, LLM Environmental Law GWU

Kurt Ettenger

Environmental Protection Specialist. Transportation Security Administration. 10 years experience. Over 2 year's experience reviewing EAs and EISs relating to security and related technology development. BA, Sociology, MA, Environmental Resource Management

Kevin T. Feeney

Environmental Protection Specialist, Environmental Planning Program Manager, Headquarters U.S. Customs and Border Protection. 20+ years experience in environmental work. Started in 1979 as a City Planner working on Master Planning and Environmental Assessments for City of Bozeman, MT. Nine years preparing Environmental Assessments and EISs. Masters of Public Administration in Urban Design and Planning,

Ms. Kebby Kelley

Lead Environmental Protection Specialist. Headquarters, United States Coast Guard. 16 years experience.

James W. McCament

Attorney, Office of the General Counsel (March 2003-August 2003), Special Advisor to the Secretary (Sept. 2003-2005). Length of time employed in profession - 6 years. Juris Doctor.

William M. McGovern

Environmental Protection Specialist. DHS Office of the Secretary (March 2003 – March 2006). 31 years experience preparing or reviewing all level of NEPA documents for several agencies, including 3 years as a team leader in EPA's Office of Federal Activities. BS in Marine Transportation, MS in Water Resources Engineering

Brent W Paul

FEMA Environmental Officer (Environmental Protection Specialist). 35 years experience (US Bureau of Reclamation, DOI and FEMA). 8 years as Agency Environmental Officer with technical oversight of 10 Regional Environmental Officers and approximately 80 environmental disaster reservists; responsible for Agency-wide environmental compliance – review of all levels of facilities NEPA documentation. BS in Engineering and MS in Systems Engineering - Water Resources Planning.

Elsa Payne

Environmental Protection Specialist. Plum Island, Science and Technology Directorate (S&T) (2003 - 2005). 7 years experience in Facilities Compliance and Site Investigation and Remediation. 2 years reviewing EAs and EISs. BS Environmental Engineering, MS Mechanical Engineering, Certified Hazardous Materials Manager, Certified Pesticide Applicator-40 Hours HAZWOPER

David Reese

Environmental Protection Specialist. Environmental Planning Program Manager at Department of Homeland Security, Management Directorate, Administrative Services, Office of Safety and Environmental Programs. 28 years of NEPA related experience preparing environmental assessments and environmental impact statements and training others in their preparation. B.S. Conservation and Natural Resources Management, M.S. Management.

Jay Roorbach

Branch Chief, Office of State and Local Government Coordination and Preparedness, Office for Domestic Preparedness, Preparedness Programs Division (2003-2005). 16 years experience.

Thomas Sheridan

Deputy Center Director, Operations. Science and Technology (S&T). 21 years experience. BS Marine Engineering, MS Operations Analysis/Systems Analysis, Nuclear Power Plant Operator Radworker 1, 40 Hours HAZWOPER

Scott Wells

Professional Forester, Detailer from the United States Forest Service / Natural Resources Manager @ Federal Law Enforcement Training Center / Environmental & Safety Division. 28 years experience in forest management, prescribed fire, law enforcement, and NEPA. 20 years experience in all phases of environmental analysis and documentation. AAS Forest Technology from the University of New Hampshire: BSF Forest Management from the University of New Hampshire: Graduate Studies in Recreation Management and Logging Engineering at Clemson University.