

U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT
ICE Policy System

DISTRIBUTION:	ICE
DIRECTIVE NO.:	1-3.0
ISSUE DATE:	October 18, 2007
EFFECTIVE DATE:	October 18, 2007
REVIEW DATE:	October 18, 2010
SUPERSEDES:	See Section 3 Below.

DIRECTIVE TITLE: ICE SCREENING CRITERIA FOR FEDERAL, STATE, OR LOCAL LAW ENFORCEMENT, CORRECTIONAL, AND MISSION SUPPORT PERSONNEL SUPPORTING ICE PROGRAMS.

1. **PURPOSE and SCOPE.** This Directive establishes U.S. Immigration and Customs Enforcement (ICE) policy regarding screening criteria for federal, state, or local law enforcement, correctional, and mission support personnel supporting ICE Programs. The provisions of this Directive define the suitability-screening standards for personnel requiring access to ICE information technology (IT) systems and the system data; or access to sensitive information (as defined herein). This Directive defines the minimum standards required for access to IT systems but is not meant to address the eligibility requirements for access to classified national security information. This Directive applies to all ICE program offices.
2. **AUTHORITIES/REFERENCES.**
 - 2.1. 8 U.S.C. § 1357(g), Performance of Immigration Officer Functions by State Officers and Employees, as amended by the Homeland Security Act of 2002 (Public Law 107-296).
 - 2.2. 10 U.S.C. § 371 *et seq.*, Use of Information Collected during Military Operations.
 - 2.3. 19 U.S.C. § 507(a)(2), Assistance to Customs Officers.
 - 2.4. Immigration and Nationality Act (INA) of 1952, Pub. L. No. 82-414, 66 Stat. 163 (codified as amended at 8 U.S.C. §§ 1101 *et seq.*) § 287(g).
 - 2.5. 5 C.F.R. Part 736, Personnel Investigations.
 - 2.6. 5 U.S.C. § 552(a), Privacy Act Issuances: 1991 Compilation, vol. II, p. 735 or Privacy Act of 1974.
 - 2.7. Department of Homeland Security (DHS) Management Directive (MD) No. 11050.2, "Personnel Security and Suitability Program".
 - 2.8. DHS Handbook 4300A, "Sensitive Security Handbook," Version 4, June 1, 2006.

ICE Screening Criteria for Federal, State, or Local Law Enforcement, Correctional, and Mission Support Personnel Supporting ICE Programs

- 2.9. Office of Management and Budget Circular No. A-130, App. III, Security of Federal Automated Information Resources, November 28, 2000.
- 2.10. DHS MD No. 1042.1, Safeguarding Sensitive but Unclassified (For Official Use Only) Information, January 6, 2005.
3. **SUPERSEDED/CANCELLED POLICY/SUMMARY OF CHANGES.** Customs Directive 1460-014A entitled, "TECS-II Access by Non-Customs Service Employee Users," issued by the former U.S. Customs Service, no longer applies to ICE. All other policy documents issued by ICE or any of its program offices on this subject prior to the date of this Directive are hereby superseded.
4. **BACKGROUND.** Customs Directive 1460-014A entitled, "TECS-II Access by Non-Customs Service Employee Users," was the primary vehicle for non-Customs employees to obtain access to information, including law enforcement sensitive information contained within the Treasury Enforcement Communications System (TECS)-II and other Information Technology (IT) Systems and Applications. Due to the creation of ICE, a consolidated ICE policy was required to encompass all ICE program offices and all law enforcement sensitive and other agency information utilized by ICE.
5. **DEFINITIONS.** The following definitions are provided for the purposes of this Directive:
- 5.1. **Candidate.** A federal, state, or local law enforcement or correctional officer, as well as any mission support personnel being considered for access to ICE IT Systems, applications, and information.
- 5.2. **ICE Facility.** DHS-owned buildings or leased space, whether for single or multi-tenant occupancy, and its grounds and approaches, all or any portion of which is under the jurisdiction, custody, or control of the Department; DHS-controlled commercial space shared with non-government tenants; DHS-owned candidate-operated facilities; and facilities under a management and operating contract such as for the operation, maintenance, or support of a Government-owned or controlled research, development, special production, or testing establishment.
- 5.3. **Information Technology (IT).** As defined by 40 U.S.C. § 11101(6)(A) ("Clinger-Cohen Act"), any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by DHS. This definition applies if the equipment is used by DHS or ICE directly or is used by a candidate under a contract with ICE that requires the use of that equipment; or of that equipment to a significant extent in the performance of a service or the furnishing of a product. The definition includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services

(including support services), and related resources.

- 5.4. **IT Systems.** Information technology systems and applications that are (1) owned, leased, or operated by ICE; (2) operated by a person on behalf of ICE; or (3) operated by another federal, state, or local government agency on behalf of ICE.
- 5.5. **Password Issuance Control System (PICS).** A system that provides password management and secure access control to DHS application system data and is overseen by the Access and Data Security Section, in ICE's Office of the Chief Information Officer.
- 5.6. **Security Activities Reporting System (SARS).** The Office of Professional Responsibility (OPR) Personnel Security Unit (PSU) tracking and data storage retrieval system.
- 5.7. **Sensitive Information.** Information, the loss, misuse, disclosure, or unauthorized access to or modification of which could adversely affect the national or homeland security interest, or the conduct of Federal programs, or the privacy to which individuals are entitled under 5 U.S.C. § 552(a) (the Privacy Act), but which has not been specifically authorized under criteria by an Executive Order or an Act of Congress to be kept secret in the interests of national defense, homeland security, or foreign policy. This definition includes the following categories of information:
 - 1) Protected Critical Infrastructure Information (PCII) as described in the Critical Infrastructure Information Act of 2002, 6 U.S.C. section 211-224; its implementing regulations, 6 C.F.R. Part 29; or the applicable PCII Procedures Manual;
 - 2) Sensitive Security Information (SSI) as described in 49 C.F.R. Part 1520; or
 - 3) Sensitive but Unclassified Information (SBU) consists of any other information which, if provided by the government, is marked in such a way to place a reasonable person on notice of its sensitive nature; or is designated "sensitive" in accordance with subsequently adopted DHS information handling requirements.
- 5.8. **Suitability.** Identifiable character traits and past conduct that are sufficient to determine whether or not a given individual is likely to carry out the duties of a job with appropriate integrity. Suitability-screening standards and determinations are distinct from security clearance standards and determinations, which address whether an individual is eligible for access to classified information.
- 5.9. **Suitability Determination.** A determination made by a personnel security specialist of an individual's fitness for access to ICE facilities, sensitive information, or resources.
- 5.10. **Suitability Screening.** The process of determining a person's suitability for employment to work or provide services to ICE or in support of ICE.

6. POLICY.

- 6.1.** To ensure the protection of ICE facilities, sensitive information, and resources, federal, state, and local law enforcement, correctional, and mission support personnel supporting ICE Programs shall undergo screening by the OPR PSU to determine their suitability to work with ICE systems, information, and resources. ICE reserves the right to restrict access to ICE facilities, sensitive information, or resources.
- 6.2.** ICE will afford fair, impartial, and equitable treatment to all individuals undergoing suitability determinations through the consistent application of suitability standards, criteria, and procedures as specified in applicable laws and regulations.
- 6.3.** Federal, state, and local law enforcement, correctional, and mission support personnel who have been vetted and approved for access to ICE IT systems prior to the issuance of this Directive are eligible to maintain their access to IT systems subject to annual recertification.

7. RESPONSIBILITIES.

- 7.1** **Director OPR** is responsible for the implementation and administration of the law enforcement, correctional officer, and mission support personnel screening program.
- 7.2** **OPR PSU Chief**, under the direction of the ICE Chief Security Officer (CSO), is responsible for suitability determinations for law enforcement, correctional, and mission support personnel supporting ICE Programs including the issuance and implementation of policies and procedures and the following:
 - 1) Designating an OPR PSU Point of Contact (POC) to assist ICE program offices in vetting federal, state, and local law enforcement, correctional, and mission support personnel supporting ICE Programs;
 - 2) Conducting, adjudicating, and tracking suitability-screening investigations and recording the determinations;
 - 3) Providing the Law Enforcement Support Center (LESC) identification data for all federal, state, and local law enforcement, correctional, and mission support personnel being vetted; and
 - 4) Notifying the ICE program offices and the National Systems Control Office (NSCO) of the results of an individual's vetting.
- 7.3** **ICE program offices** that require the use of this Directive are responsible for:
 - 1) Identifying a point of contact to work with the OPR PSU;

- 2) Identifying candidates and submitting identification and background information to the OPR PSU for processing;
- 3) Notifying the OPR PSU if a candidate for access, or an individual who has been previously granted access, has a change in status in any way; and
- 4) Notifying the sponsoring entity of the results of the suitability screening for individuals processed.

7.4 The Office of Investigations is responsible for providing the following assistance to OPR:

- 1) The NSCO is responsible for issuing, suspending, and canceling all passwords and accesses as appropriate; and
- 2) The LESC is responsible for conducting appropriate name checks when requested by OPR.

8. PROCEDURES.

8.1. Program offices will submit identification and background information for each candidate to OPR PSU in the form of a completed security packet (which includes the Standard Form (SF)-85P Questionnaire for Public Trust Positions, fingerprint cards, and access control documents).

8.2. Upon receipt of a completed security packet from a program office the OPR PSU will do the following:

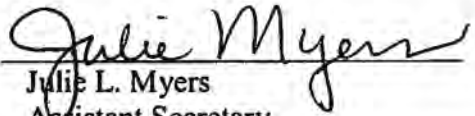
- 1) Review the SF-85P Questionnaire for Public Trust Positions;
- 2) Verify an individual's criminal history by a fingerprint check conducted through the FBI;
- 3) Conduct an LESC inquiry that includes all required law enforcement agency and immigration related checks (as required by the OPR PSU for suitability); and
- 4) Conduct an OPR Joint Integrity Case Management System check, if applicable.

8.3. Adjudication Criteria. Suitability determinations are to be made in accordance with the following adjudication criteria:

- 1) Specific factors. When making a suitability determination, the following may be considered a basis for finding an individual unsuitable:
 - a) Misconduct or negligence in employment;

- b) Criminal or dishonest conduct;
 - c) Material, intentional false statement, or deception or fraud in examination or appointment;
 - d) Refusal to furnish testimony;
 - e) Alcohol abuse of a nature and duration which suggests that the applicant or appointee would be prevented from performing the duties of the position in question, or would constitute a direct threat to the property or safety of others;
 - f) Illegal use of narcotics, drugs, or other controlled substances, without evidence of substantial rehabilitation;
 - g) Knowing and willful engagement in acts or activities designed to overthrow the U.S. Government by force; and
 - h) Any statutory or regulatory bar which prevents access to ICE systems by the candidate.
- 2) Additional considerations. In making a suitability determination, ICE shall consider the following additional considerations with regard to past conduct to the extent it is deemed pertinent to the individual case:
- a) The nature of the access for which the person is applying;
 - b) The nature and seriousness of the conduct;
 - c) The circumstances surrounding the conduct;
 - d) The recentness of the conduct;
 - e) The age of the person at the time of the conduct;
 - f) Contributing societal conditions; and
 - g) The absence or presence of rehabilitation or efforts toward rehabilitation.
- 3) A candidate may be denied access or access may be removed when the suitability determination finds that the candidate is unsuitable for the reason(s) cited above.
- 8.4. The IT Access Enrollment and Removal Procedures identified in the Appendix are to be used when issuing and removing access for civilian law enforcement, correctional, and mission support personnel.

- 8.5. The OPR PSU will conduct annual and recertification assessments to include parts or all of the above investigative requirements, as deemed appropriate, or if derogatory information is developed after systems access is granted. Individuals with access will be electronically notified of their need to be recertified.
9. **ATTACHMENTS.** Appendix, IT Access Enrollment and Removal Procedures.
10. **NO PRIVATE RIGHT STATEMENT.** This Directive is an internal policy statement of ICE. It is not intended to, and does not create any rights, privileges, or benefits, substantive or procedural, enforceable by any party against the United States; its departments, agencies, or other entities; its officers or employees; or any other person.

Approved 
Julie L. Myers
Assistant Secretary
U.S. Immigration and Customs Enforcement

Appendix

IT Access Enrollment and Removal Procedures

IT Access Enrollment Procedures: Access to ICE sensitive information by favorably adjudicated federal, state or local law enforcement, correctional, and mission support personnel supporting ICE Programs will be granted through the following process:

1. The Office of Professional Responsibility (OPR) Personnel Security Unit (PSU) will notify the respective program office that an applicant has been favorably adjudicated and will record the favorable adjudication in the Security Activities Reporting System (SARS).
2. The OPR PSU will then notify the National Systems Control Office (NSCO) that an applicant has been favorably adjudicated.
3. The NSCO, utilizing read only access to SARS, will coordinate both Password Issuance Control System (PICS) and TECS-II access for the individual to include the issuance of passwords with the respective program office.
4. The NSCO will ensure that all appropriate user records are established with the proper documentation. The NSCO will also establish and maintain the users' accounts and profiles.
5. If systems access is no longer required, or access is required to be removed as part of the reassessment/recertification, the OPR PSU will notify the NSCO for action.

IT Access Removal Procedures: When individual access to ICE sensitive information is no longer required, the following removal process shall be utilized:

1. The NSCO will deactivate and archive the access control and the user records of the individual.
2. If derogatory information is developed on an individual, the OPR PSU will be notified immediately. The PSU will then notify NSCO to ensure that all access is suspended pending a recertification.