

Department of Homeland Security (DHS)

Authorized Authoritative Credential Holder Responsibility Agreement

Department Personnel (i.e. federal employees, contractors, affiliates, retired DHS employees covered under the Law Enforcement Office Safety Act (LEOSA), and non-DHS affiliates supporting Department missions) shall sign this credential holder responsibility agreement before being issued a DHS authorized authoritative credential (e.g., DHS PIV Official [PIV-O] Pocket Credential, DHS Derived Alternate Credential [DAC], etc.). DHS authorized authoritative credentials are governed by 1) Homeland Security Presidential Directive 12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors*, 2) Federal Information Processing Standards (FIPS) Publication 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, 3) X.509 Certificate Policy for the United States (U.S.) Federal Public Key Infrastructure (PKI) Common Policy Framework, 4) DHS Directive 121-01, *Chief Security Officer*, and DHS Directive 121-03, *Common Identification Standard for DHS Employees, Contractors, Visitors, and Affiliates*, and 5) DHS Instruction *Issuance and Control of the DHS Credentials*. DHS authorized authoritative credentials are the property of the U.S. Government.

As a DHS Authorized Authoritative Credential Holder, I agree to the following:

1. I will use the DHS authorized authoritative credential for official purposes only; for DHS PIV-O Pocket Credentials, I will use it for official purposes and in accordance with the authority language printed on my PIV-O.
2. I will maintain control of my DHS authorized authoritative credential at all times and not allow anyone to use my credential for any unauthorized purpose. When not performing my official duties, I shall store my DHS authorized authoritative credential out of plain sight.
3. Based on the type of DHS authorized authoritative credential issued, I will create a Personal Identification Number (PIN) that is not easily guessable (e.g., 11111111, 12345678, etc.) or individually-identifiable in nature (e.g., Social Security Number, phone number, date of birth, etc.), and protect the PIN by not giving it to others. The PIN controls access to the private keys and information stored on a DHS authorized authoritative credential and must be protected; as such, a total of ten unsuccessful PIN attempts are given before the DHS authorized authoritative credential is locked and must be unlocked at a DHS Credentialing Facility (DCF).
4. Based on the type of DHS authorized authoritative credential issued, I will protect my private keys at all times from loss, unauthorized disclosure, or suspicion of compromise. The term "private keys" typically refers to the files that are created during a DHS authorized authoritative credential issuance/activation or maintenance (if applicable) process.
5. I will not alter or otherwise deface my DHS authorized authoritative credential. Altering or defacing includes punching a hole in, adhering decals to, or embossing the credential. I will keep my DHS authorized authoritative credential in the DHS-provided credential holder issued to me at time of credential issuance.
6. I will report changes to my employee status (e.g., federal employee, contractor, retiree, etc.); to my attribute status (e.g., emergency response official, etc.); to a change in my name; to a change in position under which the credential was originally issued, or if my DHS authorized authoritative credential is damaged or nearing expiration. When this occurs, I will report these changes to my DHS Headquarters (HQ) or Operational Component DCF location; the DHS Office of the Chief Security Officer (OCSO) HSPD-12 Program at OneCardSSD@hq.dhs.gov or (877) 807-7230; or my DHS HQ or Operational Component HSPD-12 point of contact so they can reissue the applicable new DHS authorized authoritative credential.
7. I will immediately report a compromised, lost, or stolen credential to my nearest DCF location; the DHS OCSO HSPD-12 Program at OneCardSSD@hq.dhs.gov or at (877) 807-7230; or to my DHS HQ or Operational Component HSPD-12 point of contact so they can immediately revoke the status of the credential in the Identity Management System before maintenance (e.g., reissuance, etc.) takes place to my authorized authoritative credential.
8. I understand that misuse of my DHS authorized authoritative credential includes but is not limited to any effort to coerce, intimidate, or deceive; to obtain, either directly or indirectly, any privilege, favor, preferential treatment, reward, or personal gain; attempting to bypass police-controlled checkpoints or airport security; or to avoid violations such as speeding and traffic violations (e.g., tickets, HOV violations, etc.).
9. I understand that if I misuse the DHS authorized authoritative credential issued to me, or it is compromised, lost or stolen through my noncompliance with these requirements, I may be subject to administrative or disciplinary action, or criminal and civil penalties.
10. I will surrender my DHS authorized authoritative credential to the appropriate authority (i.e. DHS HQ or Operational Component issuing agency); when my employment or association with DHS is terminated; my appointment to the position indicated on the credential is discontinued; or upon request by appropriate authority.
11. I will not violate Sections 499, 506, and 701, Title 18 of the U.S. Code through use of my DHS PIV-O PocketCredential.*

NOTE: DHS authorized authoritative credential holders must adhere to their individual Operational Component reporting requirements related to compromised, lost, and stolen property.

* 18 USC Sec. 499 says, "Whoever falsely makes, forges, counterfeits, alters, or tampers with any naval, military, or official pass or permit, issued by or under the authority of the United States, or with intent to defraud uses or possesses any such pass or permit, or personates or falsely represents himself to be or not to be a person to whom such pass or permit has been duly issued, or willfully allows any other person to have or use any such pass or permit, issued for his use alone, shall be fined under this title or imprisoned not more than five years, or both."

* 18 USC Sec. 506 says, "(a) Whoever 1) falsely makes, forges, counterfeits, mutilates, or alters the seal of any department or agency of the United States, or any facsimile thereof; 2) knowingly uses, affixes, or impresses any such fraudulently made, forged, counterfeited, mutilated, or altered seal or facsimile thereof to or upon any certificate, instrument, commission, document, or paper of any description; or 3) with fraudulent intent, possesses, sells, offers for sale, furnishes, offers to furnish, gives away, offers to give away, transports, offers to transport, imports, or offers to import any such seal or facsimile thereof, knowing the same to have been so falsely made, forged, counterfeited, mutilated, or altered, shall be fined under this title, or imprisoned not more than 5 years, or both. (b) Notwithstanding subsection (a) or any other provision of law, if a forged, counterfeited, mutilated, or altered seal of a department or agency of the United States, or any facsimile thereof, is 1) so forged, counterfeited, mutilated, or altered; 2) used, affixed, or impressed to or upon any certificate, instrument, commission, document, or paper of any description; or 3) with fraudulent intent, possessed, sold, offered for sale, furnished, offered to furnish, given away, offered to give away, transported, offered to transport, imported, or offered to import, with the intent or effect of facilitating an alien's application for, or receipt of, a Federal benefit to which the alien is not entitled, the penalties which may be imposed for each offense under subsection (a) shall be two times the maximum fine, and 3 times the maximum term of imprisonment, or both, that would otherwise be imposed for an offense under subsection (a). (c) For purposes of this section 1) the term "Federal benefit" means A) the issuance of any grant, contract, loan, professional license, or commercial license provided by any agency of the United States or by appropriated funds of the United States; and B) any retirement, welfare, Social Security, health (including treatment of an emergency medical condition in accordance with section 1903(v) of the Social Security Act (19 U.S.C. 1396b(v))), disability, veterans, public housing, education, supplemental nutrition assistance program benefits, or unemployment benefit, or any similar benefit for which payments or assistance are provided by an agency of the United States or by appropriated funds of the United States; and 2) each instance of forgery, counterfeiting, mutilation, or alteration shall constitute a separate offense under this section.

* 18 USC Sec. 701 says, "(a) Whoever manufactures, sells, or possesses any badge, identification card, or other insignia, of the design prescribed by the head of any department or agency of the United States for use by any officer or employee thereof, or any colorable imitation thereof, or photograph, print, or in any other manner makes or executes any engraving, photograph, print, or impression in the likeness of any such badge, identification card, or other insignia, or any colorable imitation thereof, except as authorized under regulations made pursuant to law, shall be fined under this title or imprisoned not more than six months, or both."

DHS Rights and Responsibilities:

1. DHS reserves the right to refuse issuance of a DHS authorized authoritative credential to any person, and such decision may be made by DHS without notice and at its sole discretion.
2. Due to the grave potential of misuse if lost, stolen, or compromised, all DHS authorized authoritative credentials are subject to inventory and inspection by the DHS HQ or Operational Component, or the DHS OCSO HSPD-12 Program, since these credentials are sensitive and high-value items.

By selecting "Enter" on the PIN pad, I acknowledge my understanding and acceptance of the terms outlined in this agreement and accept my responsibilities.

Printed Name

Signature

Date