Dams Sector

Personnel Screening Guide for Owners and Operators

Publication: 2025
Cybersecurity and Infrastructure Security Agency

Acknowledgements

The Cybersecurity and Infrastructure Security Agency (CISA), carrying out Sector Risk Management Agency (SRMA) responsibilities on behalf of the Department of Homeland Security for the Dams Sector, acknowledges the active support from the Dams Sector Coordinating Council (SCC) and Government Coordinating Council (GCC) members who contributed to the original development of *the Dams Sector Personnel Screening Guide for Owners and Operators*.

Distribution

This *Dams Sector Personnel Screening Guide for Owners and Operators* is available on the CISA Dams Sector Publications page at cisa.gov/dams-sector-publications. For additional information and details, contact the Dams Sector Management Team at DamsSector@mail.cisa.dhs.gov.

Notice

This material does not constitute a regulatory requirement, nor is it intended to conflict with, replace, or supersede existing regulatory requirements or create any enforcement standard. The statements in this document are intended solely as guidance. This document is not intended, nor can it be relied upon, to create any rights enforceable by any party in litigation.

Publication History

This document was originally published in 2009 and subsequently updated in 2017 and 2025.

Table of Contents

Introduction

The *Dams Sector Personnel Screening Guide for Owners and Operators* was developed to assist non-federal owners and operators of dams, locks, and levees in developing and implementing personnel screening protocols appropriate for their facilities. Owners and operators of federal facilities adhere to the federal government's required background investigation and Personal Identity Verification procedures. An effective screening protocol for potential employees and contractor support can contribute to enhanced facility security by ensuring that untrustworthy individuals do not gain employment or access to sensitive facilities or information.

Personnel screening protocols represent one component of a security program—the equipment, technology, personnel, and procedures designed to protect a facility against and respond to threats. Determining the need for security and protective measures starts with understanding which events could present a threat to personnel, operations, and information. Insider threat may represent one such threat of concern to Dams Sector organizations.

This guide includes a description of personnel screening objectives, sample protocols, verification methods, and additional resources to aid Dams Sector organizations in understanding and mitigating the insider threat through personnel screening. For additional information on security considerations and risk management in the Dams Sector, refer to the *Dams Sector Security Awareness Handbook* and *Dams Sector Protective Measures Handbook*, available on the Homeland Security Information Network-Critical Infrastructure (HSIN-CI) Dams Portal. For additional information on insider threats to critical infrastructure, including threat indicators and sample mitigation measures, visit CISA's Insider Threat Mitigation webpage at cisa.gov/topics/physical-security/insider-threat-mitigation.

Screening personnel involves the collection, handling, and storage of sensitive personal information and may be subject to various federal, state, and local laws. This guide is provided by CISA for informational purposes only, and implementation of any of the contents of this guide is strictly within the discretion of individual owners and operators of critical infrastructure and is not mandated by CISA. CISA disclaims any liability for any action taken in reference to the guide and this guide does not create a cause of action or any legal rights. Security incidents or threats of violence should be reported directly to your local law enforcement agency or by dialing 911.

Why Screen Personnel?

Dams, levees, and related facilities are a vital part of the nation's infrastructure, providing a wide range of economic, environmental, and social benefits through the delivery of critical water retention and control services. Security risk management in the Dams Sector considers not only the risk of failure, but also intentional acts to damage or destroy the facility or asset(s); steal materials, equipment, or information; or disrupt operations or the delivery of services. This includes risk to appurtenant structures, including powerplants and substations, pump stations, control buildings, gates, and visitor centers. Dams Sector organizations rely on a combination of employees, contractors, and vendors with varying levels of access to organizational assets—by physical and logical means—to ensure safe and secure operations and continued delivery of project benefits.

Personnel screening is the practice of developing pre-employment screening policies that identify unsuitable factors relevant to each open role, grounded in both the assessed level of risk and the operational environment. The type and level of personnel screening is conducted commensurate with the degree of harm that individuals could achieve if hired or allowed unescorted site access. The organization conducting the screening determines the scope of roles requiring screening (e.g.,

potential employees and contractors). Depending on facility specifics, visitors might also be subject to background screening. This guide addresses screening of prospective employees and contractors to minimize security risks to critical infrastructure. This guide is intended for use by owners and operators within the Dams Sector to develop screening programs that support their security goals. By implementing screening programs, owners and operators may realize other non-security benefits to their operations, such as reduced legal liability or improved operational efficiency. While these non-security benefits are highlighted briefly below, this guide is tailored to addressing security risks.

The following examples highlight three benefits of personnel screening and descriptions of unsuitable factors relevant to Dams Sector operations:

- **Identify Potential Insider Threats:** Screen applicants (e.g., potential employees and contractors) seeking unescorted site access to identify any reason(s) why they should not be hired or granted site access. Applicants could be denied employment or site access if they could pose an insider threat. Insider threat arises when employees or contractors use their knowledge of the facility, its operations, and its vulnerabilities to conduct acts of sabotage or provide sensitive information or facility access to an outsider.
- **Mitigate Potential Legal Liabilities:** Screen applicants to determine their potential to expose the employer to liability for their actions. Persons with histories of theft, assault, drug use, or other criminal offenses could pose a potential risk to employees, the public, and essential facility operations. Further, an employer could be liable for an accident caused by an employee with a known history of driving under the influence when using a facility vehicle on organization time.
- **Screen Against Job Responsibilities:** Screen applicants based on the open role's duties and responsibilities (i.e., clerical, operations, security, information technology [IT]). The basis for rejecting an application may depend on the nature of the job being sought and the applicant's background. For example, while several prior moving violations might not pose a barrier to hiring an IT professional, such violations may serve a basis for more intense scrutiny of an applicant whose responsibilities include operating facility-owned vehicles. Well-defined position descriptions or job responsibilities make it easier to determine whether or not an applicant's background is compatible with expectations of the role.

Personnel Screening Best Practices

Sample Protocols

The basic elements of a personnel screening protocol address the following questions: (1) who completes the screening, (2) what procedures are followed, and (3) what is asked of potential employees and contractors? A sample personnel screening application form is available on the Homeland Security Information Network-Critical Infrastructure (HSIN-CI) Dams Portal. Personnel screening can be managed either in-house or contracted to a reputable organization that specializes in background screening for businesses.

Regardless of who conducts the screening, carefully plan the screening procedures and questions to minimize the chance of facing legal challenges to rejected applications. For that reason, ensure all screening procedures, application forms, criteria for rejection, form-type letters, and appeal procedures have been approved by the personnel appropriate for the organization (e.g., human resources and legal counsel) to ensure compliance with state, local, and federal laws and regulations and that all applicants are treated consistently. Determine when the personnel screening

procedures and policies are documented, periodically reviewed to ensure compliance with law and mission needs, and updated as needed.

The following list represents sample best practice protocols used to screen potential employees and unescorted contractors. Further descriptions of some protocols follow the list, to aid the development of an organization's personnel screening procedures.

- Consistent use of a standard application form or specialized forms as site specifics warrant.
- Definitive and rigidly enforced policy stating which applicants must complete which forms and background checks.
- Consistently enforced policy which clearly states that failure to agree to a required background check will result in rejection of the application.
- Clearly outlined process for receiving applications, reviewing them for completeness, making acceptance or rejection decisions, documenting the decisions, and maintaining records of them.
- Precise definitions of any terms used to designate differing levels of access to facility equipment, buildings, records, computer systems, and control systems.
- Background check procedures and questions developed in compliance with applicable federal and/or state laws, any union agreements, and organization policy.
- Trained individuals to adjudicate the investigative results and issue a decision or recommendation regarding hiring of the applicant.
- Standardized acceptance and rejection form letters.
- Clearly stated criteria for which applications will be rejected.
- Precisely stated appeals process for rejected applicants.

Application Form: A formal application form is used to gather information on an applicant's identity, employment, education, criminal history, and references. When developing an application form, consider the following factors:

- **Clear Questions:** Ensure the questions used on the application form are clearly stated to elicit the information needed to make the acceptance or rejection decision. For example, the question "Have you ever violated a law?" is not likely to result in information that the employer needs to make an informed decision. A more precise query could be worded as: "Have you, since your 18th birthday, ever been convicted of violation of any law (e.g., petty misdemeanors, misdemeanors, gross misdemeanors, felonies, ordinance violations, driving while intoxicated)?" Applicants would then be asked to describe dates, locations, violations, and outcomes of any violations.
- **Consent for Screening:** Include on the application form a statement that background checks will be conducted as part of the process. Also include a section in which the applicant clearly consents to the background screening. The sample personnel screening application form on the HSIN-CI Dams Portal depicts the type of notification that could be given to potential applicants alerting them to what is involved in the screening and a consent form to be returned with the completed application.

Criteria: Clear and concise criteria for rejecting applications for employment or unescorted site access can reduce the number of claims of employment discrimination. The types of disqualification criteria potentially integrated into the screening process include misrepresented or falsified

information related to educational, employment, or criminal history; falsified identification information; positive pre-employment drug test; or employment termination elsewhere within the last two years for an action that would have been a violation of the hiring facility's safety and security principles. An example of the criteria that could be used as the basis for denying applications for employment or site access is available on the HSIN-CI Dams Portal.

Appeal Process: An appeal process for rejected applications provides a rejected applicant the opportunity and forum to correct errors in the collected information. A sample rejection letter and form that could be used as part of the appeal process are available on the HSIN-CI Dams Portal.

Reinvestigations: Reinvestigations of previously screened employees and contractors may be necessary to ensure they remain suitable for continued employment. Consider the need to add policies and procedures on reinvestigations into the organization's screening protocol. For example, reinvestigations may be triggered by time (e.g., every five years), the employee seeking a new position with the organization requiring different facility access, if new information about the employee comes to light, or after an incident.

Verification Methods

While some of the information provided by the applicant on the application form can be verified by the employer through documents supplied by the applicant, some details might need to be verified through background checks. The verification process could correspond to the following sections of a personnel screening application form:

- **Identification:** Ensure that the Social Security Number (SSN) provided is a valid number that has been issued to the applicant (i.e., the number was not issued before the applicant was born or is not in the Social Security Administration's deceased database) and that the applicant has not used other SSNs. Consider using E-Verify—administered by the Social Security Administration and the U.S. Citizenship and Immigration Services—to ascertain the validity of SSNs. E-Verify can be accessed via the webpage uscis.gov/e-verify. Also verify the authenticity of the driver's license and picture ID and that the information contained on the driver's license (e.g., age, date of birth, address) matches the details provided on the employment application form.
- **Education:** Official transcripts from educational institutions should be sufficient to verify an applicant's education history in terms of dates attended, grade point averages, and certificates/degrees awarded and years of their award. Official transcripts should carry the institution's seal and/or issued to the employer directly from the institution. The transcript should also contain the institution's accreditation status.
- **Professional Licenses and Certifications:** Verify the validity of licenses and certificates with the issuing organization. Check that the license or certificate is still valid and that no grievances, sanctions, suspensions, or other derogatory actions have been taken against the applicant.
- **Employment:** Verify that the applicant has actually been employed where and when they claimed and become aware of any employment-related information that might be relevant to the hiring decision. Verify any unexplained gaps in employment or any periods for which the applicant cannot provide sufficient explanations of their whereabouts. To the extent possible, verify that the applicant was actually employed where and for the length of time claimed; salary and job responsibilities could also be verified. Verify with an applicant's past employers any forced resignations, terminations, or actions that would make the applicant not eligible for re-employment.

- **References:** Request references from past employers. Verify the legitimacy of the references by contacting the employers and any additional references the applicant supplies.
- **Criminal History:** The number of years for which a criminal history check is conducted will depend on the applicant's proposed position and any legal limitations on the length of the check. While criminal history checks should be conducted for at least a seven-year period, individual states may not allow them beyond seven years. Elements of a criminal history check include verifying the applicant's correct date of birth, any record of felony or misdemeanor convictions, use of other names or aliases, and any pending disposition of criminal activity. Convictions, rather than arrests, can be the basis for denying employment. Consider conducting a national criminal scan by searching to identify criminal activity in jurisdictions outside of the geographical location(s) of the applicant's current and previous residences and employment.
- **Terrorist Watch:** Several lists could be checked to determine if the potential applicant has been placed on any terrorist watch lists. The lists include, but may not be limited to, the following: Department of the Treasury's Office of Foreign Assets Control Specially Designated Nationals and Blocked Persons List; the FBI's Most Wanted List; and the Interpol's Most Wanted List. Additional examples of potential lists are the United Nations Consolidated Sanctions List and the European Union Terrorist List. Employers using such watch lists as a screening device should contact the responsible agency to verify the identity of the applicant before taking any negative action on the application.
- **Motor Vehicle License/Driving Record:** This screening criterion is applicable to individuals who will be driving facility-owned or facility-leased vehicles or their own vehicles on official business. Verify that the driver's license was issued to the applicant and that the license is not under suspension or revocation. Determine if there have been any convictions within the last several years for any combination of driving under the influence/driving while intoxicated, hit and run, reckless driving, or driving with a suspended or revoked license. Verify that the applicant does not have a pattern of violating traffic laws.
- **Drug Use:** Confirm that applicants for whom drug screening is required have no positive results for the presence of drugs. Ensure that urine samples are collected in accordance with applicable regulations and that laboratories perform drug screening tests and confirmations of positive results through standard, accepted procedures (e.g., gas chromatography, mass spectrometry). Accept drug screening results only from laboratories certified by the U.S. Department of Health and Human Services.

Additional Resources

The following templates related to personnel screening are available on the HSIN-CI Dams Portal as an added resource to this guide. To access the zip file of templates, log into the portal and navigate to the *Guides* tab. For information on access requirements for HSIN-CI, contact the Dams Sector Management Team at DamsSector@mail.cisa.dhs.gov.

- Standard operating procedures for a personnel screening program
- Employment screening questionnaire (application form)
- Security screening questionnaire for board members
- Screening elements for permanent or seasonal workers
- Denial criteria and associated templates (denial letter, appeal process form)
- Rescreening questionnaire

CISA's *Resources for Onboarding and Employment Screening Fact Sheet* is designed for critical infrastructure leaders, human resources personnel, and managers of any level. This fact sheet provides actionable recommendations and resources for the vetting and employment screening of individuals, prior to their hiring into an organization. Access the fact sheet at cisa.gov/resources-tools/resources/resources-onboarding-and-employment-screening-fact-sheet.

Refer to your federal or state regulators to understand any required personnel screening procedures. For example, some organizations may be required to comply with the personnel risk assessment provisions in the North American Electric Reliability Corporation (NERC) Critical Infrastructure Program (CIP) Standard CIP-004-7, Cyber Security, Personnel and Training.