Insider Threat Potential Risk Indicators (PRI)

JOB AID

CDSE Center for Development of Security Excellence

NOVEMBER 2021

CONTENTS

Click the individual links to view each topic. You may also use the forward and backward arrows to navigate through each topic in order.

INTRODUCTION

What is an insider threat?

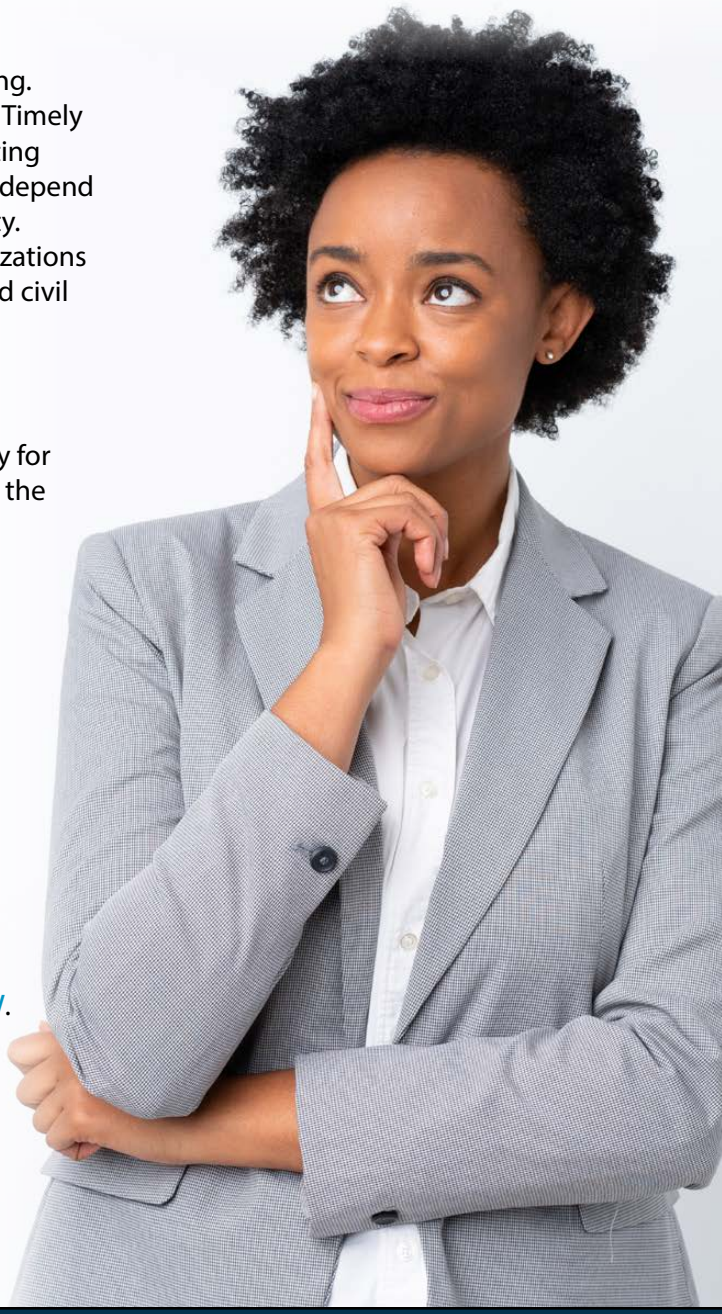
While specific definitions vary across Government, law enforcement, and industry, an insider threat is generally considered the potential for an individual to use authorized access to an organization's assets to wittingly or unwittingly do harm. The damage from insider threats can manifest as espionage, theft, sabotage, workplace violence, or other harm to people and organization. Possible insiders include employees, contractors, vendors, suppliers, and partners—anyone to whom an organization has granted special trust and access.

What are potential risk indicators (PRI)?

Individuals at risk of becoming insider threats, and those who ultimately cause significant harm, often exhibit warning signs, or indicators. PRI include a wide range of individual predispositions, stressors, choices, actions, and behaviors. Some indicators suggest increased vulnerability to insider threat; others may be signs of an imminent and serious threat.

Why are spotting and reporting PRI so important?

Indicators do not always have diagnostic value or reflect wrongdoing. Some PRI may involve activities that are constitutionally protected. Timely and appropriate reporting of PRI is crucial for assessing and mitigating insider threats. National security, critical services, and public safety depend on it. Preventing harm due to insider threat is a shared responsibility. Individuals adhere to insider threat policies and procedures; organizations investigate potential threats while preserving employee privacy and civil liberties.



For whom was this job aid created?

This job aid is for individuals who require national security eligibility for sensitive positions or access to classified information. Compared to the general public, such individuals are subject to unique standards of conduct and mandatory reporting of certain risk indicators. Special emphasis is given to PRI commonly associated with national security and the protection of classified information.

How should this job aid be used?

This job aid is not all-inclusive. Use it as a tool to develop additional PRI based on an organization's distinct mission and priorities. Utilize it also as a reminder of the exceptional duty of care vested in those with national security responsibilities. Readers should further consult applicable and controlling laws, regulations, policies, and procedures. Visit CDSE's Insider Threat Toolkit for additional training and resources at **https://www.cdse.edu/Training/Toolkits/Insider-Threat-Toolkit/**.

ACCESS ATTRIBUTES

Access is at the heart of understanding and characterizing insider threats. Without access, there is no "insider." Organizations grant individuals different kinds of access, like physical entry to buildings or virtual access to computer networks. Access may also result from specialized training, acquired skills, and organizational knowledge. Some insider threat risk is systematic or inherent: organizations cannot function without entrusting people with valuable tools and information. However, risk is lessened when sensitive access is properly assigned, managed, and protected.

Examples

- **Security clearances**
  - Confidential
  - Secret
  - Top Secret (TS)
- **Additional information controls**
  - Sensitive Compartmented Information (SCI)
  - Special Access Programs (SAP)
  - Controlled Unclassified Information (CUI)
- **Physical security access**
  - Non-public government facilities
  - Sensitive compartmented information facilities (SCIF)
  - Private sector critical infrastructure
- **Systems and applications**
  - Information network domains (SIPR, JWICS, etc.)
  - Databases and systems of record
  - Privileged accounts and credentials
  - Remote access
- **Training, tradecraft, and material**
  - Military equipment, weapons, and tactics
  - Chemical, Biological, Radiological, Nuclear, and Explosives (CBRNE)
  - Protected technology

LEARN MORE: An individual's office, position, or security eligibility alone, does not determine access to protected information. It must be necessary for the performance of one's official duties. For a short refresher on the "Need-to-Know" principle, watch the CDSE video lesson at **https://www.cdse.edu/Training/Security-Training-Videos/Personnel/Need-to-Know-Principle/**.

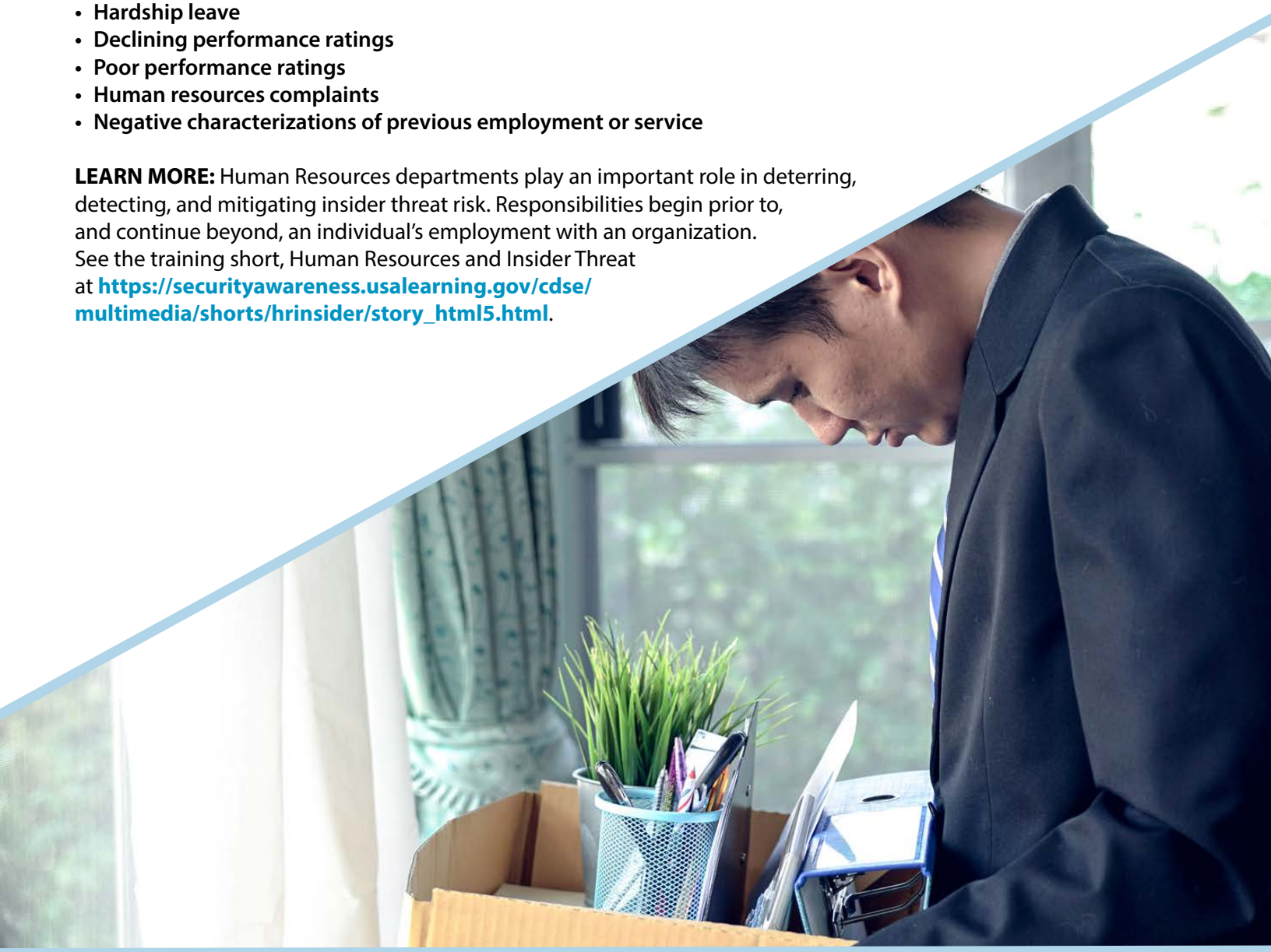
PROFESSIONAL LIFECYCLE AND PERFORMANCE

All individuals possess a unique set of characteristics and circumstances that influence their risk of becoming an insider threat. Organizational change, career progression, job performance, and other workplace dynamics can be relevant factors. Human resources personnel and supervisors are often positioned to recognize risk indicators related to professional lifecycle and performance. Some indicators may seem routine or commonplace—not everyone gets the promotion; some employees underperform, quit, or are fired—but when there is grievance, conflict, or unanticipated duress, such indicators deserve security concern.

Examples

- **Furloughs and lay-offs**
- **Separations and terminations**
- **Demotions and reprimands**
- **Non-judicial punishments**
- **Leaves of absence**
- **Unauthorized absence / AWOL**
- **Involuntary administrative leave**
- **Hardship leave**
- **Declining performance ratings**
- **Poor performance ratings**
- **Human resources complaints**
- **Negative characterizations of previous employment or service**

LEARN MORE: Human Resources departments play an important role in deterring, detecting, and mitigating insider threat risk. Responsibilities begin prior to, and continue beyond, an individual's employment with an organization. See the training short, Human Resources and Insider Threat at **https://securityawareness.usalearning.gov/cdse/multimedia/shorts/hrinsider/story_html5.html**.



SECURITY AND COMPLIANCE INCIDENTS

The proper handling and safeguarding of protected information is crucial to combating many insider threats such as fraud, theft, and espionage. Protected information includes proprietary information, in addition to classified and other sensitive Government information. All individuals with access have a duty to adhere to rules and regulations for protected information. Compliance failures are a security concern whether they are deliberate or not—insider threats are frequently the result of negligence. Risk indicators include security and compliance violations, unauthorized use or disclosure, and any inappropriate efforts to view or obtain protected information outside one's need to know.

Examples

- **Violations related to the handling of protected information**
  - Disclosure to unauthorized persons (e.g. personal or business contacts, media)
  - Unauthorized collection, retention, or storage
  - Using unauthorized equipment or mediums for protected information
  - Attempts to obtain information without proper clearance or need-to-know
  - Unauthorized modification of information to conceal or remove classification, or control markings
- **Negligent or lax physical or information security practices despite counseling**
- **Non-compliance with security training requirements**
- **Security clearance denial, suspension, or revocation**
- **Failure to self-report information required for security clearance eligibility**
- **Misuse of information security privileges or credentials**
- **Misuse of facilities or work-issued equipment**
- **Anomalous or suspicious accessing of facilities or systems during non-work hours**

LEARN MORE: Security procedures for storing sensitive material include proper facilities, containers, and labels. In some instances, guards and alarm systems are mandatory. Requirements for protection increase with sensitivity. Take the training short, Classified Storage Requirements at **https://securityawareness.usalearning.gov/cdse/multimedia/shorts/csr/story_html5.html**.

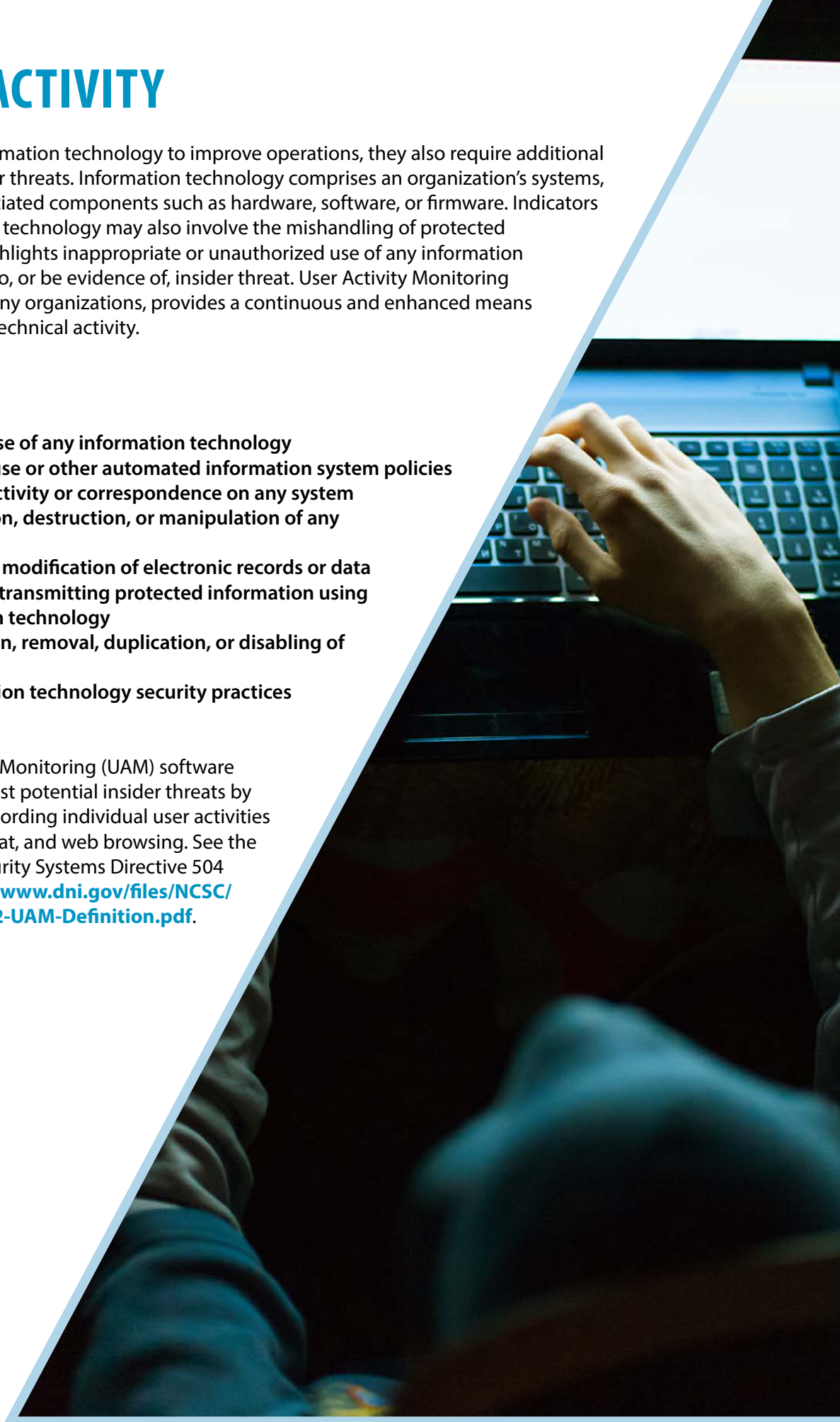
TECHNICAL ACTIVITY

As organizations adopt information technology to improve operations, they also require additional safeguards to prevent insider threats. Information technology comprises an organization's systems, networks, devices, and associated components such as hardware, software, or firmware. Indicators of the misuse of information technology may also involve the mishandling of protected information. This section highlights inappropriate or unauthorized use of any information technology that could lead to, or be evidence of, insider threat. User Activity Monitoring (UAM), a requirement for many organizations, provides a continuous and enhanced means of detecting and recording technical activity.

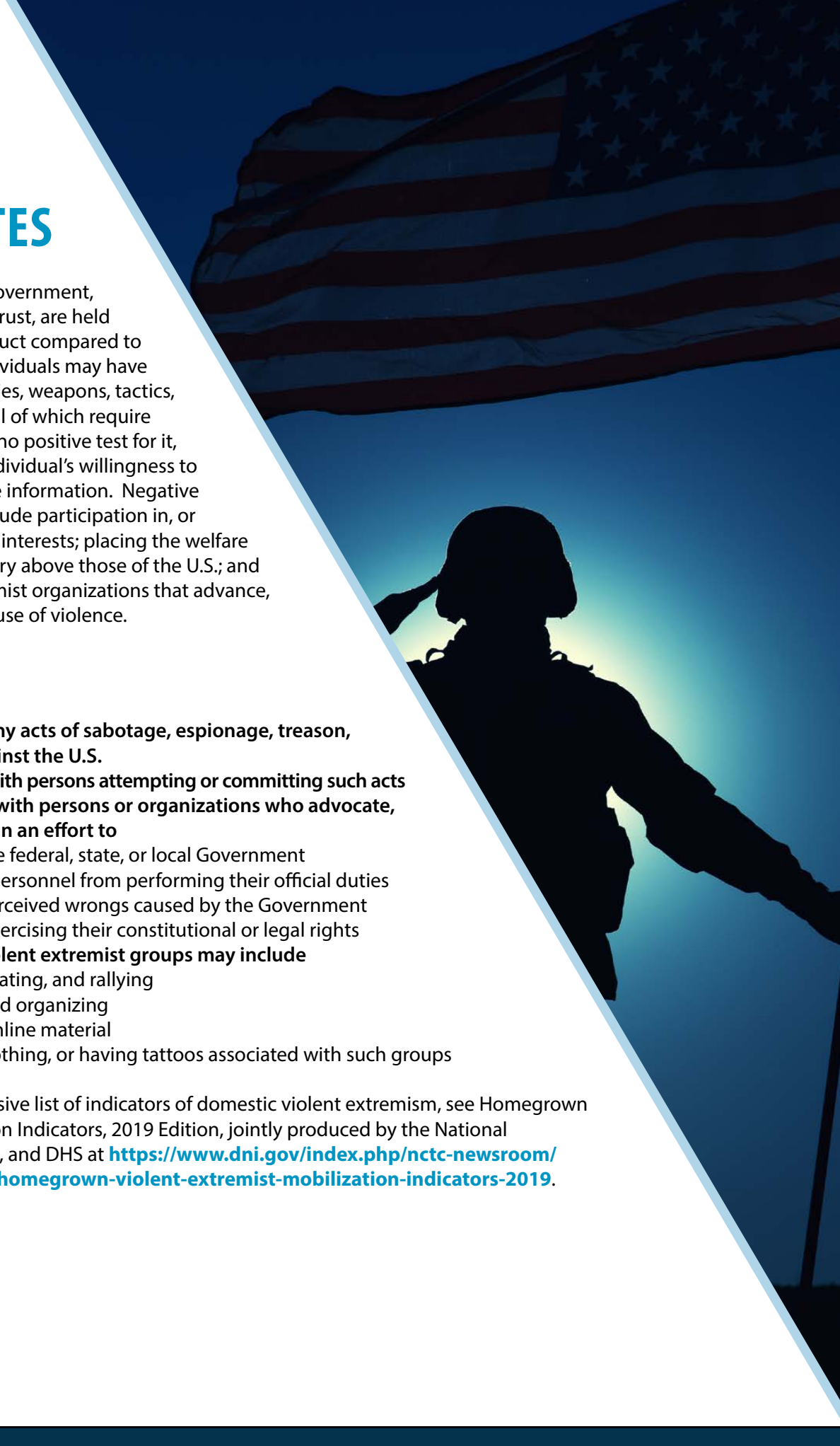
Examples

- **Unauthorized access or use of any information technology**
- **Violations of acceptable use or other automated information system policies**
- **Suspicious or improper activity or correspondence on any system**
- **Unauthorized modification, destruction, or manipulation of any information technology**
- **Unauthorized deletion or modification of electronic records or data**
- **Downloading, storing, or transmitting protected information using unauthorized information technology**
- **Unauthorized introduction, removal, duplication, or disabling of software on any system**
- **Negligent or lax information technology security practices despite counseling**

LEARN MORE: User Activity Monitoring (UAM) software protects organizations against potential insider threats by monitoring, logging, and recording individual user activities such as keystrokes, email, chat, and web browsing. See the Committee on National Security Systems Directive 504 definition of UAM at **https://www.dni.gov/files/NCSC/documents/nittf/20181022-UAM-Definition.pdf**.



ALLEGIANCE TO THE UNITED STATES



Individuals in the military, Government, or other positions of public trust, are held to a higher standard of conduct compared to the general public. Such individuals may have access to Government facilities, weapons, tactics, training and intelligence—all of which require safeguarding. While there is no positive test for it, allegiance may dictate an individual's willingness to protect classified or sensitive information. Negative indicators are broad and include participation in, or support for, acts against U.S. interests; placing the welfare or interests of another country above those of the U.S.; and active participation in extremist organizations that advance, encourage, or advocate the use of violence.

Examples

- **Support or advocacy of any acts of sabotage, espionage, treason, terrorism, or sedition against the U.S.**
- **Association or sympathy with persons attempting or committing such acts**
- **Association or sympathy with persons or organizations who advocate, threaten, or use violence in an effort to**
  - Overthrow or influence federal, state, or local Government
  - Prevent Government personnel from performing their official duties
  - Gain retribution for perceived wrongs caused by the Government
  - Prevent others from exercising their constitutional or legal rights
- **Active participation in violent extremist groups may include**
  - Fundraising, demonstrating, and rallying
  - Recruiting, training, and organizing
  - Distributing print or online material
  - Knowingly wearing clothing, or having tattoos associated with such groups

LEARN MORE: For an expansive list of indicators of domestic violent extremism, see Homegrown Violent Extremist Mobilization Indicators, 2019 Edition, jointly produced by the National Counterterrorism Center, FBI, and DHS at **https://www.dni.gov/index.php/nctc-newsroom/nctc-resources/item/1945-homegrown-violent-extremist-mobilization-indicators-2019**.

FOREIGN INFLUENCE AND PREFERENCE

Foreign associations may exist for a variety of reasons, including familial ties or work duties. Foreign contacts and interests rise to a national security concern when they result in divided or conditional U.S. allegiance. They also pose risk if they create vulnerability to foreign manipulation, coercion, or pressure to act against U.S. interests. Contacts from countries linked to terrorism or known to target U.S. citizens for intelligence operations may be of particular concern. Foreign involvement, such as possessing or seeking foreign citizenship, while not inherently harmful, is a security concern when an individual expresses foreign preference over U.S. interests or attempts to conceal such involvement.

Examples

- **Foreign travel to countries of concern**
- **Frequent unofficial foreign travel**
- **Foreign, unofficial contact with a known or suspected foreign intelligence entity (FIE)**
- **Enabling or facilitating an officer, agent, or member of a FIE**
- **Continuing foreign national contact (to include personal contact, telephone, email, social media)**
  - bonds of affection
  - intimate contact
  - exchange of personal information
- **Foreign business and political interests**
- **Foreign residency or property interests**
- **Foreign bank accounts and sources of income**
- **Possession of a foreign passport or identity card**
- **Voting in a foreign election**
- **Service in a foreign military or government**
- **Application for and receipt of foreign citizenship**
- **Foreign national cohabitant or roommate**

LEARN MORE: Individuals must report certain activities, including foreign travel and contacts, for initial and continued national security eligibility. For specific requirements, refer to the Security Executive Agent Directive (SEAD)-3, Reporting Requirements; and SEAD-4, National Security Adjudicative Guidelines at **https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-security-executive-agent/ncsc-policy**.

OUTSIDE ACTIVITIES

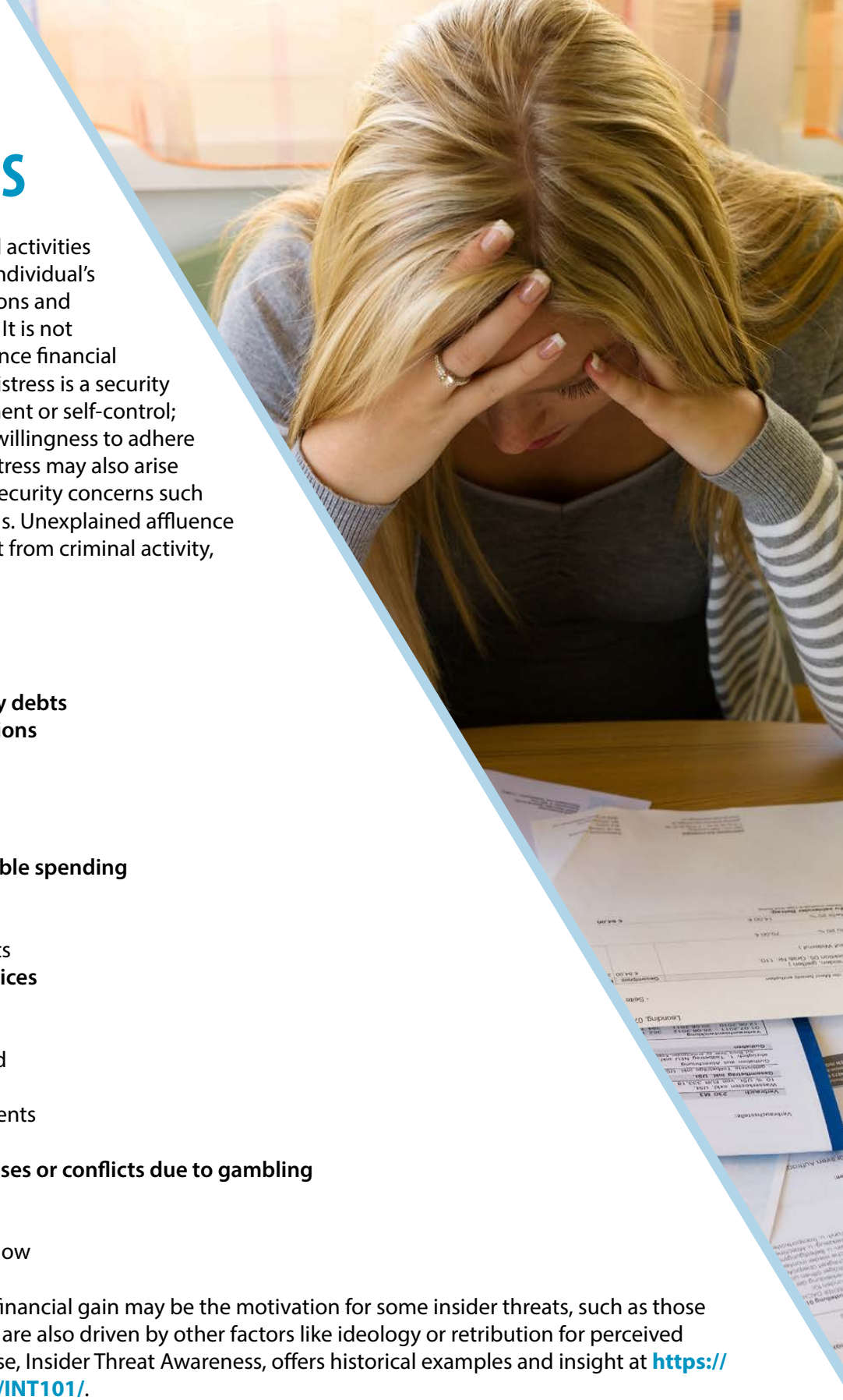
An individual who engages in outside employment or services, whether on a volunteer or paid basis, does not represent an inherent threat. However, outside activities are a security concern if they pose a conflict of interest with an individual's security responsibilities. Any involvement in outside activities that increases the risk of unauthorized disclosure of protected information is of particular concern. While potential risk indicators may have foreign considerations, they also include outside activities with U.S. organizations or persons, especially when it involves matters of national security or sensitive technology. Failure to fully disclosure outside activities when required is also cause for concern.

Examples

- **Foreign employment or service**
  - Government of a foreign country
  - Any foreign national or organization
  - Representative of any foreign interest
- **Any employment or service involving analysis, discussion, or publication of**
  - Intelligence
  - National defense
  - Foreign Affairs
  - Protected Technology
- **Concealment or failure to fully disclose outside activities**

LEARN MORE: Individuals are generally permitted to engage in outside activities that pose no conflict with official duties, but should first consult with the appropriate ethics office. The Department of Defense Standards of Conduct Office provides guidance for active duty and civilian personnel at **https://dodsoco.ogc.osd.mil/DoD-Personnel/Ethics-Topics-for-DoD-Personnel/Outside-Activities/**.

FINANCIAL CONSIDERATIONS



Personal finances and finance-related activities may have substantial bearing on an individual's suitability for holding sensitive positions and safeguarding protected information. It is not uncommon for individuals to experience financial loss or hardship. However, financial distress is a security concern when indicates poor judgement or self-control; or it impairs an individual's ability or willingness to adhere to rules and regulations. Financial distress may also arise because of, and thus indicate, other security concerns such as gambling and substance addictions. Unexplained affluence is pertinent to the extent it may result from criminal activity, including espionage.

Examples

- **Inability or unwillingness to satisfy debts**
- **History of unmet financial obligations**
  - Pay garnishment
  - Loan defaults
  - Liens or judgements
  - Bankruptcy
- **Evidence of frivolous or irresponsible spending**
  - Excessive debt
  - Significant negative cash flow
  - Late payments or non-payments
- **Deceptive or illegal financial practices**
  - Embezzlement
  - Employee theft
  - Check or expense account fraud
  - Mortgage or tax fraud
  - Intentional financial misstatements
- **Failure to file or pay income taxes**
- **Significant transactions, debts, losses or conflicts due to gambling**
- **Unexplained affluence**
  - Lifestyle or standard of living
  - Increases in net worth or cash flow

LEARN MORE: While the promise of financial gain may be the motivation for some insider threats, such as those involving espionage or theft, insiders are also driven by other factors like ideology or retribution for perceived grievances. The CDSE eLearning course, Insider Threat Awareness, offers historical examples and insight at **https://www.cdse.edu/Training/eLearning/INT101/**.

SUBSTANCE MISUSE AND ALCOHOL CONSUMPTION

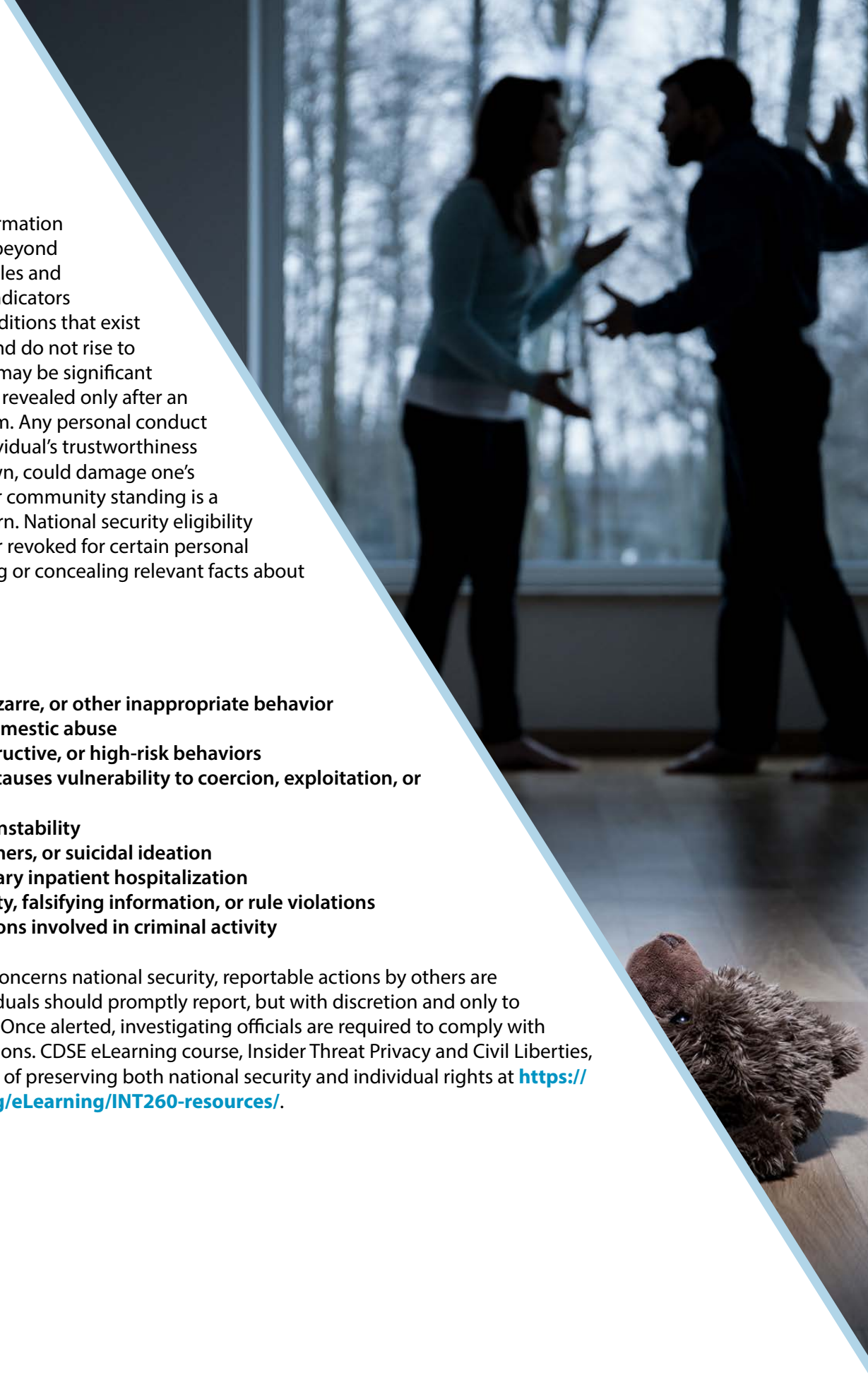
The illegal use of controlled substances demonstrates an individual's inability or unwillingness to comply with laws, rules, and regulations. Substance misuse further raises concerns about an individual's reliability and trustworthiness because such behavior may also result in physical or psychological impairment. Alcohol, while not illegal, can similarly increase the risk of insider threat when it is consumed inappropriately, excessively, or abusively. Alcohol-related incidents may be security concerns whether they occur at, or away from, the workplace.

Examples

- **Illegal drug use while granted access to classified information or holding a sensitive position**
- **Illegal possession of a controlled substance, including drug paraphernalia**
- **Misuse of prescription and non-prescription drugs**
- **Drug test failures or refusals**
- **Qualified diagnosis of substance use disorder**
- **Alcohol-related incidents away from work (e.g. drinking and driving, disturbing the peace, spouse or child abuse)**
- **Alcohol-related incidents at work (e.g. reporting for duty intoxicated, drinking on the job)**
- **Habitual or binge drinking to the point of impaired judgement**
- **Voluntary or involuntary treatment for drug or alcohol abuse**
- **Failure to follow court orders regarding drug or alcohol education, evaluation, treatment, or abstinence**

LEARN MORE: Alcohol and substance use disorders, mental health, and financial issues are life challenges for which an organization's Employee Assistance Program (EAP) may be of significant value. EAPs can mitigate insider threat risk by providing timely and critical support to individuals. The U.S. Office of Personnel Management provides more information about federal programs at **https://www.opm.gov/policy-data-oversight/worklife/employee-assistance-programs/**.

PERSONAL CONDUCT



Access to protected information imparts responsibilities beyond compliance with work rules and regulations. Some risk indicators involve behaviors or conditions that exist outside the workplace and do not rise to criminal conduct. These may be significant but under-reported, and revealed only after an insider causes grave harm. Any personal conduct that undermines an individual's trustworthiness and reliability; or, if known, could damage one's personal, professional, or community standing is a pertinent security concern. National security eligibility is normally not denied or revoked for certain personal conduct, but for falsifying or concealing relevant facts about the conduct in question.

Examples

- **Disruptive, violent, bizarre, or other inappropriate behavior**
- **Family conflict and domestic abuse**
- **Compulsive, self-destructive, or high-risk behaviors**
- **Sexual behavior that causes vulnerability to coercion, exploitation, or duress**
- **Emotional or mental instability**
- **Self-harm, harm to others, or suicidal ideation**
- **Voluntary or involuntary inpatient hospitalization**
- **A pattern of dishonesty, falsifying information, or rule violations**
- **Association with persons involved in criminal activity**

LEARN MORE: When it concerns national security, reportable actions by others are broadly inclusive. Individuals should promptly report, but with discretion and only to the appropriate officials. Once alerted, investigating officials are required to comply with privacy laws and regulations. CDSE eLearning course, Insider Threat Privacy and Civil Liberties, examines the challenges of preserving both national security and individual rights at **https://www.cdse.edu/Training/eLearning/INT260-resources/**.

CRIMINAL CONDUCT

Not surprisingly, criminal conduct raises doubts about an individual's reliability and trustworthiness to hold sensitive positions and safeguard protected information. On its face, it demonstrates the inability or unwillingness to comply with laws, rules, and regulations. Potential risk indicators of a criminal nature do not require formal criminal charges or prosecution; credible allegations or admissions are sufficient. Minor offenses (certain traffic offenses, for example) are unlikely indicators of insider threat, unless they contribute to a pattern or combination of offenses that causes concern about an individual's trustworthiness, reliability, or judgement.

Examples

- **Criminal violent behavior**
- **Sexual assault and domestic violence**
- **Weapons-related crimes**
- **Parole or probation or violation thereof**
- **Failure to follow court orders**
- **Credible allegations or reports of criminal activity**
- **Admissions of criminal activity**
- **A pattern or combination of minor criminal offenses**
- **Military discharge or dismissal for reasons less than "Honorable"**

LEARN MORE: Different responsible parties may best ascertain the risk of an insider threat at different times. Qualified investigators and adjudicators gather risk indicators and assess individuals for national security eligibility determinations. In other instances, insider threats are mitigated only when vigilant individuals observe and report potential risk indicators. For examples of recent insider threats, and the risk indicators associated with each, explore the CDSE Case Study Library at **https://securityawareness.usalearning.gov/cdse/case-studies/index.php**.