INTERAGENCY SECURITY COMMITTEE

Managing Risk of Adverse/Involuntary Employee Separations

An Interagency Security Committee Guide

2024 Edition

U.S. Department of Homeland Security
Cybersecurity and Infrastructure Security Agency
Interagency Security Committee

Change History and Document Control

Rev. #	Date	Changes	Approver
1.0	7/20/23	Initial Draft	ISC
2.0	TBD	Initial Issue	ISC

Document Control

The ISC authorizes distribution of this document to federal, state, local agencies, and private individuals or enterprises.

Message from the Interagency Security Committee

The Interagency Security Committee (ISC) provides leadership and guidance for security programs to help safeguard the nonmilitary federal community. Over the years, observers have noted that the involuntary separation of a federal employee or federal contractor worker due to adverse or other administrative actions may pose risk.

Due to the risk of workplace violence or other undesirable events from involuntarily separated employees, the ISC captured best practices from across the federal government and private sector that organizations should consider before, during, and after the separation of an employee. While difficult to predict how an employee will respond, it is possible to mitigate risk with the use of an effective threat assessment and risk management strategy. Separating an employee properly and having a plan reduces the risk to the organization, employees, government property, and information systems.

This guide provides best practices on how to conduct an employee separation risk assessment and categorize that risk, keys to success for notifying the employee, managing access to facilities and information technology (IT) systems, remote worker considerations, and post-separation vigilance. This guide also offers recommendations for a risk-based removal and exiting security checklist.

This document is not all-inclusive as each separation is unique. In addition, federal laws and regulations govern employee separations. Therefore, it is important the organization's security element develops organization policy and collaborates with human resources (HR), including employee relations and labor relations, management (supervisor), legal, contracts, grants, and visitor management, as needed, to enhance and customize the risk mitigation best practices described in this document.

Table of Contents

Introduction

Managing the risk associated with separating an employee[1] is not a one size fits all proposition. Involuntary separations due to adverse or other administrative actions pose greater risk. In these instances, tailor the separation or removal process to decrease the organization's exposure to risk. Federal laws and regulations govern employee separations. Therefore, it is important the organization's security element develops organization policy and collaborates with human resources (HR), including employee relations and labor relations, management (supervisor), legal, contracts, grants, and visitor management, as needed, to enhance and customize the risk mitigation best practices described in this document.

Due to the risk of workplace violence or other undesirable events from involuntarily separated employees, the Interagency Security Committee (ISC) Best Practices Subcommittee (hereafter Subcommittee)[2] developed recommendations for consideration before, during, and after the separation of an employee. Separating an employee properly and having a plan reduces the risk to the organization, employees, government property, and information systems.

Managing Risk of Adverse/Involuntary Employee Separations: An Interagency Security Committee Guide provides best practices on how to conduct an employee separation risk assessment and categorize that risk; keys to success for notifying the employee and managing access to facilities and information technology (IT) systems; remote worker considerations; and post-separation vigilance. This guide also offers recommendations for a risk-based removal and exiting security checklist.

NOTE: *If a threat of violence is imminent, call 911, notify the appropriate law enforcement agency, and inform applicable internal and external security partners immediately.*

[1] This guide uses the term "employee" throughout to describe federal employees and federal contractor workers.

[2] The ISC Best Practices Subcommittee evaluates technology solutions, develops guidance on lessons learned and information sharing, and maintains a clearinghouse of information for federal security programs. Departments and agencies should tailor this guidance based on their own requirements and site-specific needs.

1. Pre-Separation

Federal laws and regulations govern employee separations. Sometimes the separation process can be lengthy, and it is important to synchronize any security or risk management actions to ensure they are complementary to the employee separation process.

The process should treat employees facing separation with dignity and respect. It is important to recognize the separation of an employee is a stressful situation for management, staff, and the employee. Developing a concise plan and timeline, which includes time and place of notification of separation, will assist in providing a smooth transition. It is also important during this time to use communications with the employee to inform the threat assessment team[3] as they begin to assess risk. Before communication with any bargaining unit employee, the threat assessment team should work with the agency labor relations staff to determine whether the employee qualifies for union representation.

Keep accurate records for GFE, PIV, and access cards issued to employees.

Many organizations have an existing threat assessment team as part of their Workplace Violence or Insider Threat Programs. It is a best practice to have a threat assessment team who can provide input and information to conduct a risk assessment, determine the risk level, and identify appropriate actions to take during a Moderate[4] or High-Risk[5] separation. Recommended members for the threat assessment team include, HR, management, legal, security, internal oversight offices (e.g., Inspector General, Office of Professional Responsibility), and a behavioral analyst or psychologist (if available). Other entities that may also be appropriate, depending on the circumstances, include contracts, grants, visitor management, and Office of Civil Rights/Equal Employment Opportunities for additional information. Share information only on a need-to-know basis.

Provide guidance to management on how to identify concerning behaviors and include specific steps they should take to report a risk or perceived threat to people, property, or data.

[3] This guide uses the term "threat assessment team" throughout to describe a multi-disciplinary group of individuals who can help assess an employee separation and provide recommended mitigation actions.

[4] A "moderate risk separation" can result from a voluntary or involuntary separation. See Table 1.

[5] A "high-risk separation is usually the result of performance or behavioral concerns. See Table 1.

1.1. Risk Assessment

A risk assessment is critical before, during, and after the separation of the employee to minimize potential for an undesirable response. Identify risk factors based on behavior of the employee and the reason for the separation. **Appendix A: Separation Risk Assessment** outlines an example risk assessment process, identifies recommended risk categories, and recommends the development and implementation of a risk management strategy during separation. **Table 1** identifies several example employee separation types and the possible associated risk level categories: Low, Moderate, or High Risk.

A key component in determining the risk level is identifying and assessing the employee's past and present behavior. Each employee separation type can move up or down on the levels of risk given any unique risk factors identified prior to a separation. For example, even involuntary administrative separations can generate highly emotional responses. **Appendix A: Separation Risk Assessment** outlines general questions to assist the threat assessment team in determining the risk level and recommends appropriate measures to mitigate behavioral risk concerns before, during, and after the separation of the employee.

Table 1: Example Risk levels associated with different types of employee separations

Risk Level	Employee Situation
Low	Retirement
Low	Voluntary resignation (no pending investigation or performance issues)
Low	Employee-led transfer to another organization
Moderate	Voluntary resignation (pending investigation or performance issues)
Moderate	Abandonment — has not come to work and contact has been unsuccessful
Moderate	Employer-led transfer to another organization
Moderate	Layoff due to budget cuts or workforce Reduction in Force
Moderate	Completing assigned period
Moderate	Administrative — Involuntary removal due to non-security reasons *(i.e., using department/agency resources for personal benefit)*
High	Involuntary Separation for security reasons (i.e., sharing confidential information, criminal activity, etc.)
High	Performance-related removal *(i.e., incompetence, insubordination, or attendance issues)*
High	Behavioral concerns including theft, substance abuse, sexual harassment, workplace violence, fraud, angry outburst, etc.
High	Separation because of a substantiated investigation

2. Separation

Employee separations are a sensitive and difficult task, and it is important to handle the process with care and professionalism. Removal of the employee's physical access to the facility and logical access to systems must coincide closely with the separation meeting for Moderate and High-Risk separations. **Appendix B: Removal/Exiting Security Checklists** provides an example checklist for use during the separation process at each of the risk level categories.

Maintain an adverse separation contact list. Consult with legal and other internal resources, such as human resources, to develop approved communications, such as email templates, for notifying points of contact (POCs) in the case of a high-risk separation. Communications should provide a synopsis of the threat, timeline for separation (including employee notification), and specific requests for each government POC (e.g., revoke system access, disable PIV card, and send requests for returned equipment).

Key during the separation is maintaining dignity and respect for the employee. Understand the employee's situation by conducting a risk assessment (see **Appendix A: Separation Risk Assessment**) and developing a plan to best support the employee and the organization. Based on the risk assessment and the employee's status (i.e., are they remote? Are they on administrative leave?) an agency, based on their policies and procedures, may choose to issue the notification of separation, rights of the employee, and any other instructions by mail or another delivery method.

The actual separation of an employee from a workplace carries a risk that is unpredictable and possibly disruptive. Personnel should be prepared. Here are some general best practices for separation that the necessary parties should coordinate:

1. **Plan and prepare for the notification of separation meeting:**
   - Consider the best people to deliver the notification of separation. Keep participants to a minimum but not less than two individuals, preferably individuals from outside the employee's immediate work group, other than the individual's supervisor.
   - Before the meeting, prepare a written separation letter outlining the reasons for the separation and the next steps. Also, ensure all necessary documents, such as the employee's contract, performance evaluations, and any relevant HR or security policies are prepared before the meeting.
   - Notify IT and the Security Office of the date and time of the notification of separation meeting and remove all physical and logical access at an appropriate time based on risk. Remove the ability of the employee to access systems remotely.

2. **Conduct the meeting in a private, safe, and respectful location:**
   - Choose a quiet and private location where you can discuss the separation without interruptions or distractions. Pick a location away from high traffic areas, where people naturally congregate, and away from the employee's immediate colleagues.
   - If possible, pick a location near an exterior wall and exit. Arrange seating to ensure those delivering the news can exit if necessary.
   - Have a place outside of the room for personal belongings such as backpacks, coats, etc. Do not allow these items into the room.
   - Begin the meeting by expressing your appreciation for the employee's contributions, if applicable and if it will not compromise an administrative or investigative action. Alternatively, acknowledge the time the employee has been with the organization.
   - Explain the reason for the separation in a timely, clear, and concise manner.
   - Consider having building security notified if there is potential for an adverse reaction.
3. **Be honest, empathetic, and non-combative:**
   - Communicate the decision with honesty and empathy and avoid blaming or criticizing the employee.
   - Listen to their perspective and respond with compassion and understanding.
   - Avoid responding to or allowing a separated employee to lure an argument.
4. **Provide clear information about post-separation arrangements:**
   - Discuss the employee's final paycheck, severance pay (if applicable), health benefits (if applicable), and any other post-separation arrangements which are applicable. Where possible and if applicable, extend benefits to help the employee achieve a less stressful transition. Understand the employee may take some time to process the notification of separation and may not be able to absorb a lot of information. A best practice is to provide this information in written form for the employee to consider later.
   - Answer questions and provide a copy of the separation letter and any relevant documents.
   - Prepare and communicate a plan for the employee's personal belongings if located in the organization's facility. If allowing the employee to gather belongings, consider the day and time to preserve dignity and minimize risk. Do not allow unescorted access. Consider mailing personal belongings to the employee in a manner that is secure, insured, and provides proof of delivery and acceptance.

5. **Recover Documents and Government Furnished Equipment (GFE):**
   - Prepare a plan for handling the return of department and agency documents and processing those documents once collected or returned.
   - Obtain GFE, credentials, card readers, Personal Identity Verification (PIV) Cards, keys, IT systems, and any other identification cards, building or parking passes and remove employee from access control system(s).
6. **Respect confidentiality:**
   - After the separation, respect the employee's privacy and confidentiality by not discussing the details of the separation with other employees. However, organizations should inform team members and key personnel the employee has separated to prevent unauthorized access and encourage reporting if the employee tries to return.

The following real-world example in **Case Study 1** illustrates a scenario in which revoking network access was an important step in mitigating risk before a high-risk employee separation.

Case Study 1: Revoking Access before a High-Risk Employee Separation

In July 2022, an employee with authorized access to a stand-alone government communications network used granted access to download and delete system security files.

Network security detected the activity and started remediation actions.

ACCESS DENIED

While on administrative leave, the person of interest attempted to gain access to the government network by requesting a username and password exemption; the request was denied. The employee was then separated.

Source: The Risk Management Process, Appendix A: The Design-Basis Threat Report

Follow protocols for processing timely badge returns, especially for high-risk separations. Protocols should establish timeline requirements to require written confirmation of requests to revoke a contract employee's access to systems and facilities.

2.1. Separation Considerations for Remote Employees

Remote employee separations should follow the same general guidelines as identified for in-person separations. In addition to considering the nature of the separation, some remote considerations include location of remote employee, distance from office(s), access to a facility, logical access, and issued government equipment. Whenever possible conduct the notification of separation meeting in person or virtually with the remote employee. An agency may choose to issue the separation notice, and any instructions restricting the employee's access, by mail or another delivery method. As a result, an agency may determine a meeting with the employee is not necessary.

Consider the risk level when developing the plan on how to notify the employee of the separation. If a moderate or high-risk separation employee can telework, there is increased opportunity to do damage by downloading information. The removal of logical or physical access may need to occur at the time of notification of separation.

Removing physical access to the facility(s), logical access to systems, and, if appropriate, notifying security and managers may be more imperative because it may take longer or become more difficult to collect a remote employee's government identification and GFE. If this occurs for federal civil service employees, the agency should determine if it is necessary to place the employee in an administrative leave status pending any decision on separating the employee from federal service.

Some additional considerations include:

1. **Virtual Challenges:** There can be technical issues such as poor internet connection, video conferencing software malfunctions, and other communication problems which can make the process more complicated while conducting the notification of separation of a remote employee. Communication may be more difficult during the separation of a remote employee, as it may be more challenging to read nonverbal cues and respond to feedback. This can make it more challenging to ensure the employee fully understands the reasons for their dismissal and the next steps in the process.
2. **Security and Privacy Concerns:** The notification of separation meeting may involve sensitive government information or proprietary data which may be more difficult to manage access to for an employee who is receiving the information remotely. When separating an employee in a remote environment, it may be more challenging to ensure confidentiality, and not compromise the employee's privacy if the employee is working from home.
3. **Special Considerations:** Federal laws and regulations, as well as individual agency policies, may require specific procedures for separating remote employees, which can add additional coordination and planning (i.e., the retrieval of GFE, credentials, card readers, PIV Cards, keys, IT systems, and any other identification cards, building or parking passes for potentially hostile remote employees).

2.2. Separation Considerations for Federal Contractor Workers

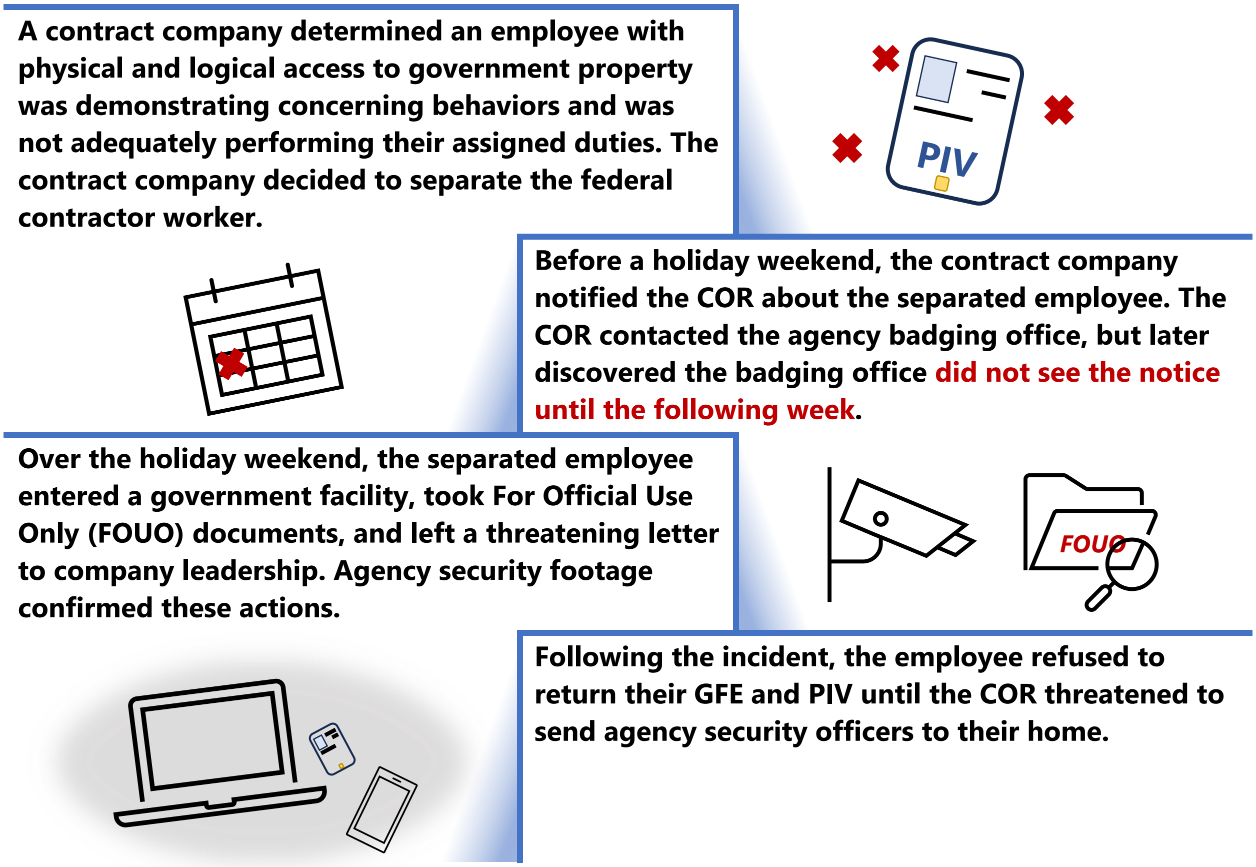
A federal contractor worker is an employee of the contract company and not a federal employee. Therefore, the separation of a federal contractor worker is the responsibility of the contract company. In general, standard language in the contract should articulate the contract company shall notify the government of all separations and resignations within a specific timeframe and include the Contracting Officer Representative (COR) in all discussions. It is the responsibility of the contract company to facilitate the prompt return of all GFE, credentials, card readers, PIV Cards, keys, IT systems, and any other issued identification cards, building or parking passes that may have been issued to the COR or the appropriate government security office. If not retrieved, the separated employee could potentially still access government facilities or information systems, presenting a greater risk. The contract company should also develop a risk-based separation protocol for low-, medium-, and high-risk separations. The protocol should include procedures to ensure comprehensive communication and coordination with corporate, partner, and government stakeholders.

NOTE: Immediate removal of physical access to facility(s), logical access to systems, and, if appropriate, notification to the facility security, and/or employees should occur when a contract company conducts a moderate or high-risk separation.

In addition, the agency should establish separation processes and procedures outlining the agency requirements and policy for the separation of federal contractor workers. If there is no agency separation policy or procedure in place, recommend the COR obtain support from the contract company to establish guidelines and communication expectations concerning the separation of a federal contractor worker. In support of Homeland Security Presidential Directive 12 (HSPD-12) compliance, contracting companies should develop a risk-based separation protocol and incorporate the considerations listed in **Appendix B: Removal/Exiting Security Checklists** which provides security related activities for employee separations. This should include the mechanism or protocols for contacting or convening the threat assessment team for moderate or high-risk separations.

The following real-world scenario in **Case Study 2** illustrates the risk linked to involuntary employee separations for contracting companies.

Case Study 2: High-Risk Federal Contractor Worker Separation



A contract company determined an employee with physical and logical access to government property was demonstrating concerning behaviors and was not adequately performing their assigned duties. The contract company decided to separate the federal contractor worker.

Before a holiday weekend, the contract company notified the COR about the separated employee. The COR contacted the agency badging office, but later discovered the badging office did not see the notice until the following week.

Over the holiday weekend, the separated employee entered a government facility, took For Official Use Only (FOUO) documents, and left a threatening letter to company leadership. Agency security footage confirmed these actions.

Following the incident, the employee refused to return their GFE and PIV until the COR threatened to send agency security officers to their home.

Source: Partner Forces, LLC. "Evaluating Risk during Contractor Separations." (2024).

3. Post-Separation Vigilance

Risk management for adverse or involuntary separations does not end with removal. A separated employee can still present risk. Separated employees may return for a variety of reasons—both benign and threatening. For this reason, it is important to maintain vigilance post-separation. Remaining vigilant can involve HR, management, security, and sometimes peers or colleagues. Provide post-separation observations to the threat assessment team to enable them to adjust the risk management strategy accordingly.

Post-separation vigilance best practices include:

1. The results of any follow up by HR or other organization staff (e.g., manager), if follow up is appropriate and in accordance with agency policies, to assess the separated employee’s demeanor.
2. Encourage peers and colleagues to report the former employee if they communicate any threatening or harassing messages. If available, periodically review camera coverage of the exterior of the facility during and after hours.
3. Immediately report any moderate or high-risk separated employee who returns to the facility to security.
4. If security personnel initially received notification of the separation through a Be On the Lookout (BOLO) alert, periodically check to ensure they have relevant information, such as the individual’s car make and model and license, and the finite period of time to maintain this alert.
5. Train employees on how to recognize concerning or suspicious behaviors and activity and the importance of security awareness (i.e., no piggybacking, presentation of badges, awareness of surroundings, etc.).

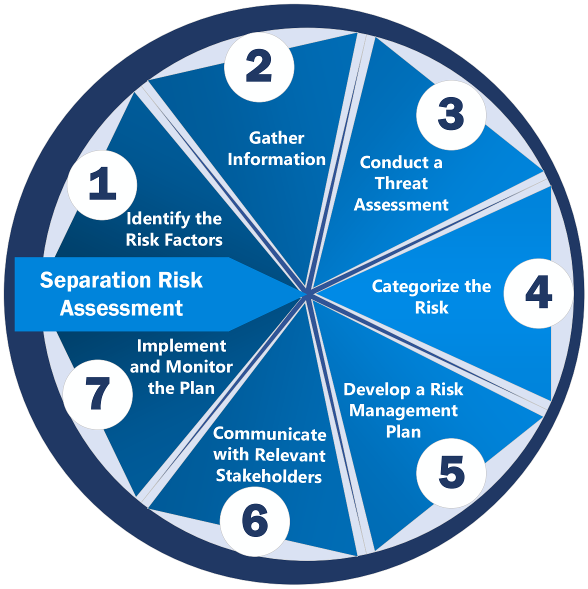
Stick to post-separation procedures to safeguard information and reduce overall risk to people, property, and data. Post-separation procedures may include reviewing security camera footage and tracking employee GFE, PIV, or building access card usage, while still in their possession. Security personnel should follow "be on the lookout" (BOLO) procedures for 2-3 months following any high-risk employee separations.

4. Conclusion

The ISC developed this guide in response to several of its members requesting guidance on how to best manage risk for adverse or involuntary separations. Each employee separation scenario will be a little different. However, this guide provides best practices on how to conduct an employee separation risk assessment and categorize that risk; keys to success for notifying the employee and managing access to facilities and IT systems; remote worker considerations; and post-separation vigilance. This guide also offers recommendations for a risk-based exiting checklist.

The following appendices offer step-by-step guidance on conducting a separation risk assessment and a removal/exiting security checklist both of which are risk-based.

Appendix A: Separation Risk Assessment


1
Identify the Risk Factors
2
Gather Information
3
Conduct a Threat Assessment
4
Categorize the Risk
5
Develop a Risk Management Plan
6
Communicate with Relevant Stakeholders
7
Implement and Monitor the Plan
Separation Risk Assessment

Designing a separation risk assessment process involves seven key steps. This includes identifying the risk factors, gathering information, conducting a threat assessment, categorizing the risk, developing a risk management plan, communicating with relevant stakeholders, and implementing and monitoring the plan. The assessment should focus on the individual, and not only the reason for the separation, but also their behavior, history, and the overall circumstance of the departing employee.

Many federal agencies have established threat assessment teams within their Insider Threat Program or Workplace Violence Program, a multi-disciplinary group of individuals who can help assess the separation and provide recommended mitigation actions. The threat assessment team is a vital part of the adverse/involuntary separation of an employee by considering the security and safety of the organization and ensuring implementation of risk mitigation security measures, while observing and following laws and regulations and respecting the rights of the individual.

The following steps are not all inclusive but assist in creating a risk assessment framework for adverse/involuntary separation of employees:

Step 1: Identify the Risk Factors

Identify the specific risk factors associated with the employee and the separation. These may include the employee's job function, access to sensitive information, history of threatening or violent behavior, and the reason for the separation.

- Is the person leaving voluntarily (retirement, other position, etc.) or involuntarily (performance, reduction in force, behavior, policy violation, etc.)?
- Could the employee possess unique knowledge/information (security clearance, access to systems, etc.) to retaliate against the agency?
- Has the employee reacted negatively to disciplinary actions in the past?
- Has the employee presented behavior risk concerns?
- Has the employee shown other concerning behavior changes?
- Has the employee targeted the organization, supervisors, or coworkers through threatening social media posts?
- Does the employee have access to weapons?
- Has the employee experienced any personal stresses (i.e., financial difficulties, divorce, loss of family member or friend, etc.)?
- Does the employee have a personal support unit (family)?
- Have coworkers expressed concerns about the person’s temperament, change of habits, or any out of the ordinary behavior?

NOTE: The above list is not all inclusive but provides a baseline for the threat assessment team to begin an evaluation.

Step 2: Gather Information

It is imperative to gather information from relevant sources, including HR, management, security specialists, and co-workers, to gain a full understanding of the employee's behavior and identify potential risks.

- Do coworkers describe the employee as combative, hot-headed, or hard to work with?
- Do coworkers describe the employee as a loner, non-social or having recently changed to exhibit non-social behaviors?
- Does the employee have friends at work?
- Is the employee local to the facility?
- What is the relationship between the employee and their supervisor?
- How long has the employee worked for the organization?
- Does the employee have a violent criminal history?
- Has there been any recent reports of violent criminal activity (i.e., assaults, domestic violence, etc.) involving the employee?
- Does the employee have a history of using violence or having large outbursts to resolve conflict?
- Does the employee carry a firearm into the workplace that would activate removal procedures for disarming and recovering firearms?
- If available, what is the employee posting on social media? Are they targeting the organization, supervisors, or coworkers through threatening posts?

NOTE: The above list is not all inclusive but provides a baseline for the threat assessment team to work from.

Step 3: Conduct a Threat Assessment

Conduct a threat assessment to evaluate the likelihood and severity of potential threats posed by the employee. This may involve analyzing the employee's history, behavior, and motivations, as well as the likelihood of retaliation or violent behavior.

Step 4: Categorize the Risk

A **'low-risk'** separation is generally the result of the employee leaving the organization due to retirement or securing new employment. There is no indication the employee may become resentful or pose a threat.

A **'moderate-risk'** separation can result from a voluntary or involuntary separation. If there is reasonable cause for concern, such as prior performance concerns or behavioral issues, the separation categorizes as a 'moderate-risk'.

A '**high-risk'** separation refers to the separation of an employee who is likely to pose a risk of harm to themselves or others. High-risk separations are usually a result of performance or behavioral concerns. The risk can be highest at the time of separation, or in the hours or days surrounding the removal. HR, management, and security specialists should be attentive to the potential for violence prior to, and following, any separation.

Step 5: Develop a Risk Management Plan

Develop a risk management plan which will outline measures to mitigate any identified risks. This may include security measures such as, increasing monitoring or changing access to sensitive information, notifying law enforcement or other relevant authorities, or implementing a protective order.

Step 6: Communicate with Relevant Stakeholders

Within privacy constraints, be sure to communicate with relevant stakeholders, HR, management, and security, to ensure everyone is aware of the potential risks and the risk management plan.

Step 7: Implement and Monitor the Plan

Leadership should implement and monitor the risk management plan to ensure it is effective in mitigating all identified risks. Once implemented, it will be critical to continue to monitor the situation and adjust the plan, as needed.

Appendix B: Removal/Exiting Security Checklists

The following checklist ***is a guide*** for security related activities for removals/exits of employees and contractors and does not address all offboarding processes or procedures. It is important to involve relevant security and IT personnel in the separation process to address all security-related concerns. Agency specific information regarding removals or separations may supersede this guide.

Note*: The specific separation actions for a contractor will depend on the terms of their contract and the circumstances surrounding their separation.* The contract company may keep the employee on their staff, but the federal contract must remove the contract employee from the federal contract.

High Risk		
Action	**Date**	**Supervisor's Initials**
Notify relevant offices, such as HR, Employee Labor Relations, payroll, and benefits, of the removal/separation.		
Conduct risk assessment.		
Notify appropriate security disciplines, as needed.		
Notify the individual's supervisor if they are not already aware of the removal/separation. Ensure the supervisor understands their role and responsibilities in the transition.		
Ensure trained personnel conduct exit interview. Exit interviews should cover the following key points: • Discuss the reason for separation. • Gather feedback from the employee. • Provide information about the employee's entitlements. • Review the employee's continuing obligations, including safeguarding confidential government information. Employees with NSI shall receive a debriefing and sign appropriate forms. • Verify the employee understands the terms of their removal/separation.		
Revoke access to classified information, including security clearances and access to secure facilities, **immediately upon separation notification**, or as per HR and Security department guidelines.		
Disable all access to government systems and facilities within **1 hour** of the individual's separation notification.		
Ensure the individual returns all government property, including GFE, credentials, card Readers, PIV Cards, keys, IT systems, and any other identification cards, building or parking passes within **1 hour** of the individual's separation notification.		

Recover department and agency documents within **1 hour** of the individual’s separation notification.		
Notify IT staff to terminate the individual's computer and email accounts within **1 hour** of the individual’s separation notification.		
Ensure the proper documentation of all records related to the individual's separation and maintain for future reference.		

Certification

Supervisory Acknowledgment: (Completed by Separating Employee’s/Contractor’s Supervisor).

I have reviewed the obligations and responsibilities listed in the parts above, including the employee's certification of return of all material, equipment, property, and official files or papers, and I am satisfied the employee has met their responsibilities for separation.

____________________________________ _______________________

Signature Date

Moderate Risk

Action	Date	Supervisor’s Initials
Notify relevant offices, such as HR, Employee Labor Relations, payroll, and benefits, of the separation.		
Conduct risk assessment.		
Notify appropriate security disciplines, as needed.		
Notify the individual's supervisor if they are not already aware of the separation. Ensure the supervisor understands their role and responsibilities in the transition.		
Ensure trained personnel conduct exit interview. Exit interviews should cover the following key points: • Discuss the reason for separation. • Gather feedback from the employee. • Provide information about the employee’s entitlements. • Review the employee’s continuing obligations, including safeguarding confidential government information. Ensure the debriefing of employees with NSI and sign appropriate forms. • Verify the employee understands the terms of their separation.		
Revoke access to classified information, including security clearances and access to secure facilities, **immediately upon separation notification**, or as per HR and security department guidelines.		
Disable all access to government systems and facilities within **4 hours** of the individual’s separation notification.		

Ensure the individual returns all government property, including GFE, credentials, card readers, PIV Cards, keys, IT systems, and any other identification cards, building or parking passes within **4 hours** of the individual's separation notification.		
Recover department and agency documents within **4 hours** of the individual's separation notification.		
Notify IT staff to terminate the individual's computer and email accounts within **4 hours** of the individual's separation notification.		
Ensure the proper documentation of all records related to the individual's separation and maintain for future reference.		
Certification		
Supervisory Acknowledgment: (Completed by Separating Employee's/Contractor's Supervisor). I have reviewed the obligations and responsibilities listed in the parts above, including the employee's certification of return of all material, equipment, property, and official files or papers, and I am satisfied the employee has met their responsibilities for separation. ______________________________ ____________________ Signature Date		

Low Risk		
Action	**Date**	**Supervisor's Initials**
Notify relevant offices, such as HR, Employee Labor Relations, payroll, and benefits, of the separation.		
Notify appropriate security disciplines, as needed.		
Notify the individual's supervisor if they are not already aware of the separation. Ensure the supervisor understands their role and responsibilities in the transition.		
Ensure trained personnel conduct exit interview. Exit interviews should cover the following key points: • Discuss the reason for separation. • Gather feedback from the employee. • Provide information about the employee's entitlements. • Review the employee's continuing obligations, including safeguarding confidential government information. Ensure the debriefing of employees with NSI and sign appropriate forms. • Verify the employee understands the terms of their separation.		

Revoke access to classified information, including security clearances and access to secure facilities, within **18 hours** of the individual’s last day.		
Disable all access to government systems and facilities within **18 hours** of the individual’s separation.		
Ensure the individual returns all government property, including GFE, credentials, card readers, PIV Cards, keys, IT systems, and any other identification cards, building or parking passes within **18 hours** after the individual’s last day.		
Recover department and agency documents within **18 hours** after the individual’s last day.		
Notify IT staff to terminate the individual's computer and e-mail accounts within **18 hours** of the individual’s last day.		
Ensure the proper documentation of all records related to the individual's separation and maintain for future reference.		

Certification

Supervisory Acknowledgment: (Completed by separating employee’s/contractor’s supervisor).

I have reviewed the obligations and responsibilities listed in the parts above, including the employee's certification of return of all material, equipment, property, and official files or papers, and I am satisfied the employee has met their responsibilities for separation.

_______________________________ _______________________

Signature Date

***Note**: The timeframes provided in these checklists are general guidelines and may vary depending on the specific organizational policies and security requirements. It is essential to consult with HR, Legal, and Security departments to establish precise timeframes for each risk level and ensure compliance with applicable regulations.*

Appendix C: References

List of Abbreviations/Acronyms/Initialisms

Abbreviation	**Full Name of Term**
BOLO	Be On the Lookout
COR	Contracting Officer Representative
GFE	Government Furnished Equipment
HR	Human Resources
ISC	Interagency Security Committee
IT	Information Technology
PIV	Personal Identification Verification

Glossary of Terms

Term	Definition
Adverse Separation	An employee separated involuntarily from employment based on conduct or performance.
Facility	Space built or established to serve a particular purpose. The facility is inclusive of a building or suite and associated support infrastructure (e.g., parking or utilities) and land.
Federal Contractor Worker	According to 11 C.F.R. § 115.1 "a person, as defined by 11 C.F.R. § 100.10, who enters into a contract with the United States or any department or agency thereof for the rendition of personal services; or furnishing any material, supplies, or equipment; or selling any land or buildings; if the payment for the performance of the contract or payment for the material, supplies, equipment, land or building is to be made in whole or part from funds appropriated by Congress.”
Federal Departments and Agencies	Those executive departments enumerated in 5 United States Code (U.S.C.) § 101, independent establishments as defined by 5 U.S.C. § 104(1), Government corporations as defined by 5 U.S.C. § 103(1), and the U.S. Postal Service.
Federal Employee	An employee, as defined in section 2105 of title 5, United States Code, of an agency.

Term	Definition
Government Furnished Equipment (GFE)	Government-furnished property means property in the possession of, or directly acquired by, the Government and subsequently furnished to the contractor for performance of a contract. Government-furnished property includes, but may include more than, spares and property furnished for repair, maintenance, overhaul, or modification. Government-furnished property also includes contractor-acquired property if the contractor-acquired property is a deliverable under a cost contract when accepted by the Government for continued use under the contract. Equ*ipment* means a tangible item that is functionally complete for its intended purpose, durable, nonexpendable, and needed for the performance of a contract. The government does intend for equipment to be for sale and does not ordinarily lose its identity or become a component part of another article when put into use. Equipment does not include material, real property, special test equipment or special tooling.
Human Resources (HR)	The Human Resources department (HR department, sometimes just called "Human Resources") of an organization performs human resource management, overseeing various aspects of employment, such as compliance with labor law and employment standards, interviewing and selection, performance management, administration of employee benefits, organizing of employee files with the required documents for future reference, and some aspects of recruitment (also known as talent acquisition) and employee offboarding. They serve as the link between an organization's management and its employees.
Information Technology	Any equipment, interconnected system, or subsystem of equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency.
Involuntary Separation	The dismissal from employment due to the actions or decisions of the employer and not the employee.
Level of Risk	The combined measure of the threat, vulnerability, and consequence posed to a facility from a specified undesirable event.
PIV Card	An identification card issued by a federal agency that contains a computer chip, which allows it to receive, store, recall, and send information in a secure method. The main function of the card is to encrypt or code data to strengthen the security of both employees’ and Veterans’ information and physical access to secured areas, while using a common technical and administrative process.
Removal	A separation from Federal service initiated by the agency, the Office of Personnel Management or the Merit Systems Protection Board under parts 359, 432, 731, or 752 of title 5, Code of Federal Regulations; section 1201 of title 5, U.S. Code; or comparable agency statutes or regulations. (Note: This Chapter covers actions that remove an employee from the agency. Most removals from the Senior Executive Service under part 359 result in conversion to an appointment outside the Senior Executive Service.
Risk	A measure of potential harm from an undesirable event encompassing threat, vulnerability, and consequence.

Term	Definition
Risk Assessment	The process of evaluating credible threats, identifying vulnerabilities, and assessing consequences.
Risk Management	A comprehensive approach to allocating resources for the protection of a facility, assets, and occupants to achieve an acceptable level of risk. Risk management decisions are based on the application of risk assessment, risk mitigation, and-when necessary-risk acceptance. Extended definition: Process of identifying, analyzing, and communicating risk and accepting, avoiding, transferring or controlling it to an acceptable level at an acceptable cost. Annotation: The primary goal of risk management is to reduce or eliminate risk through mitigation measures (avoiding the risk or reducing the negative effect of the risk), but also includes the concepts of acceptance and/or transfer of responsibility for the risk as appropriate. Risk management principles acknowledge that, while organizations cannot eliminate, they can usually take actions to reduce risk.
Risk Management Strategy	A proactive approach to reduce the usually negative impacts of various risks by choosing within a range of options that include complete avoidance of any risk that would cause harm or injury, accepting the risk, controlling the risk by employing risk mitigation options to reduce impacts, or transferring some or all of the risk to another entity based on a set of stated priorities.
Risk Mitigation	Extended definition: Course of action or actions to be taken in order to manage risks; proactive approach to reduce the usually negative impacts of various risks by choosing within a range of options that include complete avoidance of any risk that would cause harm or injury, accepting the risk, controlling the risk by employing risk mitigation options to reduce impacts, or transferring some or all of the risk to another entity based on a set of stated priorities. Sample usage: Mutual aid agreements are a risk management strategy used by some emergency response authorities to respond to large scale incidents. The application of strategies and countermeasures to reduce the threat of, vulnerability to, and/or consequences from an undesirable event. Extended definition: Application of measure or measures to reduce the likelihood of an unwanted occurrence and/or its consequences. Organizations may implement measures prior to, during, or after an incident, event, or occurrence. Example: Risk mitigation greatly reduced the potential impact of the tsunami on the local population. Annotation: Organizations may implement measures prior to, during, or after an incident, event, or occurrence.

Term	Definition
Separation	The cessation of employment relationship. The DHS Lexicon Terms and Definitions 2017 Edition – Revision 2 includes the types of separation: resignations (leaving government and moving to another government agency), retirements (disability, mandatory, voluntary, full retirement, involuntary, etc.), removals, death, reduction in force or RIF, terminations, etc.
Tailgating	Tailgating, sometimes referred to as piggybacking, is a type of physical security breach in which an unauthorized person follows an authorized individual to enter secured premises.
Threat	The intention and capability of an adversary to initiate an undesirable event.
Undesirable Event	An incident adversely impacting facility occupants or visitors, operation of the facility, or mission of the agency.
Voluntary Separation	An employee's decision to leave a job on their own accord. An employee may choose to leave a job for a wide variety of reasons. An especially common reason for voluntary separation is leaving for a new and better job, typically one that offers higher remuneration or improved career prospects.
Weapon	An object, such as a club, knife, or gun, used to injure, defeat, or destroy.

References

Cybersecurity and Infrastructure Security Agency

- Insider Threat Mitigation Guide, November 2020
- Pathway to Violence

Department of Homeland Security

- National Threat Evaluation and Reporting: Basic Threat Evaluation and Reporting Course

Executive Order

- Executive Order 14111

Federal Bureau of Investigation

- A Study of Pre-Attack Behaviors of Active Shooters in the United States Between 2000 and 2013

Interagency Security Committee

- Planning and Response to an Active Shooter: An Interagency Security Committee Policy and Best Practice Guide, 2021 Edition
- Violence in the Federal Workplace: A Guide for Prevention and Response, 2019 Edition

Investopedia

- What is Voluntary Termination? Definition, Causes, and Process

National Institute of Standards and Technology

- Personal Identity Verification (PIV) of Federal Employees and Contractors

Sean A. Ahrens, CPP, CSC

- Involuntary Employment Separation/Termination Strategies V2

Security Industry Association

- Involuntary Employment Separation Strategies V2

TechTarget

- Tailgating (Piggybacking)

1) **Department of Homeland Security** – Office of Intelligence and Analysis National Threat Evaluation and Reporting Office (Basic Threat Evaluation and Reporting) dated July 2022.

United States Secret Service National Threat Assessment Center

- Mass Attacks in Public Spaces: 2016 - 2020

Acknowledgements

Best Practices Subcommittee

Brian Grogan
Chair
Department of Energy

Contributing Authors

Samantha Hintz
U.S. Secret Service

Robert Pauley
U.S. Citizenship & Immigration Services

Subcommittee Members

Gean Alston
Department of Homeland Security

Anthony Cardwell
Department of Homeland Security

Mitch Dowdy
Department of Commerce

Michael England
Nuclear Regulatory Commission

Mark Gaouette
General Services Administration

Michael Griffin
General Services Administration

Jennifer Hammen
Department of Homeland Security

Roger Hansel
Internal Revenue Service

Christopher Huza
Department of Health and Human Services

Chad Hyland
U.S. Patent and Trade Office

Donell Jones
Department of Health and Human Services

David Kelly
Department of Health and Human Services

Kelly Kester
Department of the Treasury

Charles King
Drug Enforcement Administration

Quinn Knight
Customs and Border Protection

Hoa Ly
U.S. Capitol Police

Nicholas Mikalis
Department of Homeland Security

Lorne Murphy
Department of the Treasury

Christopher Scott
Pentagon Force Protection Agency

Charles Sembly
Department of Health and Human Services

Michael Sparks
Department of Energy

Renee Speare
Internal Revenue Service

AJ Washington
Department of Commerce

Interagency Security Committee

Daryle Hernandez

Tarvis Bonner
Management and Program Analyst

Katrina Brasfield
Policy Analyst

Robert Chaiet
Technical Editor

Kevin Choate
ISC Regional Advisor,
Regions 6 & 8

Scott Dunford
Senior Security Specialist

Shawn Fiebiger
Deputy Program Manager

Harrison Heller
Operations Research Analyst

Scott Hochenberg
Public Outreach and Messaging
Subject Matter Expert

Martin Kobylarczyk
Management Analyst

Elizabeth Rhee
Public Relations Specialist