REF-IR-01: Incident Response Playbook

📊 DATA TABLE LOCATION

The data table for this register is maintained in the Excel file:

REF-IR-01_Incident_Response_Playbook_v2.0.xlsx

Use the Excel file for data entry and record-keeping.
This Word document provides instructions and guidance.

Step-by-Step Procedures for Common Security Incidents

Document ID: REF-IR-01 **Version:** 2.0 **Classification:** CUI (contains security procedures and contact information) **Parent Policy:** POL-IR-06 (Incident Response Plan) **Last Updated:** [DATE] **Document Owner:** Chief Information Security Officer (CISO)

---

1. PURPOSE & OVERVIEW

Document Purpose

This Incident Response Playbook provides detailed, step-by-step procedures for responding to common cybersecurity incidents. It enables rapid, effective response by providing pre-defined workflows for incident handlers, reducing decision-making time during high-stress situations.

Key Functions: - Provides actionable procedures for 8 common incident scenarios - Documents DFARS 252.204-7012 72-hour reporting requirements - Defines roles and responsibilities during incidents - Guides evidence collection and preservation - Supports NIST SP 800-171 control 3.6.1 (Incident Handling) - Ensures consistent, repeatable incident response

Scope

This playbook covers: - **Incident detection and triage** - **Containment procedures** (immediate actions to limit damage) - **Eradication procedures** (removing threat actor/malware) - **Recovery procedures** (restoring normal operations) - **Post-incident activities** (lessons learned, improvements)

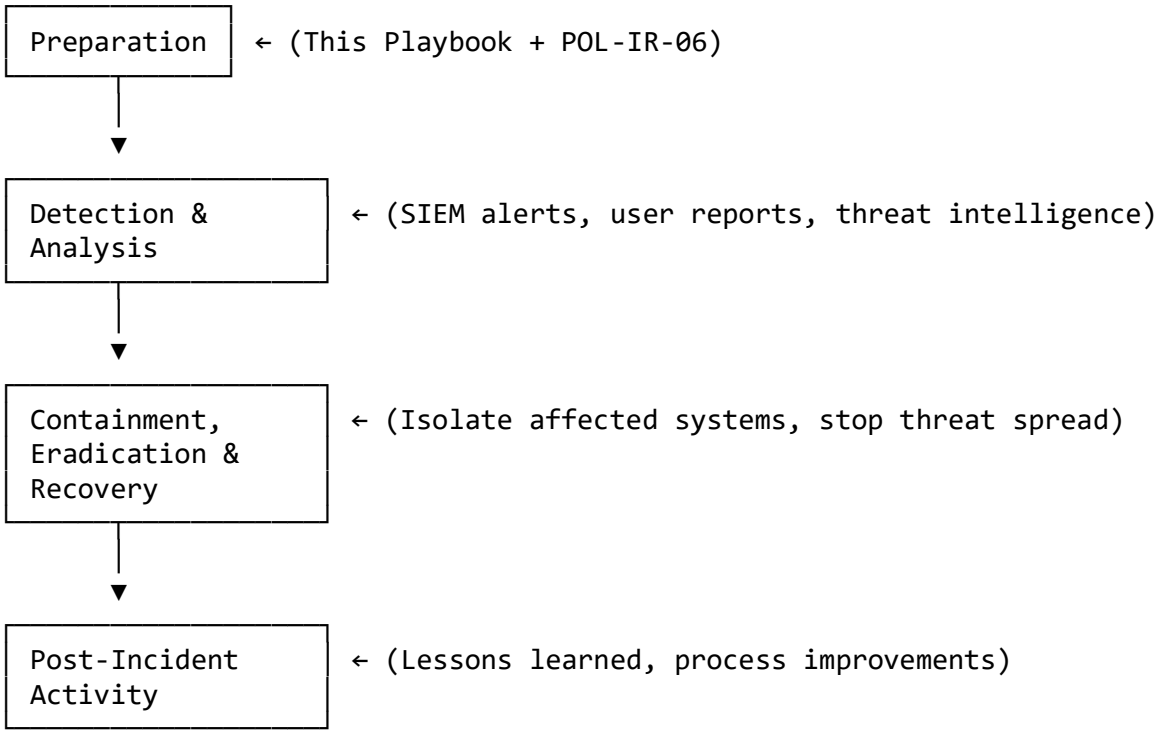
Out of Scope: - Disaster recovery procedures (see POL-CP-15 Contingency Planning) - Business continuity procedures (see REF-CP-05 Contingency Plan) - Physical security incidents (see POL-PE-10 Physical Security)

---

2. INCIDENT RESPONSE FRAMEWORK

2.1 NIST SP 800-61 Incident Response Lifecycle

This playbook follows the NIST SP 800-61 Rev 2 incident response lifecycle:



2.2 Incident Severity Classification

2.3 Incident Response Team Roles

After-Hours Contact: - **Security Hotline:** [PHONE NUMBER] (24/7 on-call rotation) - **Incident Email:** security-incident@[COMPANY].com - **Emergency Escalation:** [CISO MOBILE], [CTO MOBILE]

2.4 DFARS 252.204-7012 Reporting Requirements

Covered Defense Information (CDI) / CUI Cyber Incident Reporting:

When a cyber incident affects CUI or systems that process CUI, contractors **MUST report to DoD within 72 hours**.

Reporting Criteria: - CUI was actually or potentially compromised (accessed, stolen, modified) - Malware was discovered on a CUI system - Unauthorized access to a CUI system occurred - Denial of service prevented access to CUI

How to Report: 1. **Immediately (within 72 hours):** Submit report via DoD Cyber Crime Center (DC3) portal - Portal: https://dibnet.dod.mil - Include: Incident description, date/time discovered, affected systems, CUI involved 2. **Follow-Up:** Provide

media/forensic images if requested by DoD 3. **Document:** Log all DoD reporting in REF-IR-02 Incident Log

Key Point: The 72-hour clock starts when you **discover** the incident, not when it occurred. Report promptly even if investigation is ongoing.

---

3. COMMON INCIDENT SCENARIOS

SCENARIO 1: Ransomware / Malware Infection

Incident Description: Ransomware encrypts files and demands payment; other malware may steal data, install backdoors, or cause system damage.

Detection Indicators: - File extensions changed (e.g., .encrypted, .locked, .crypted) - Ransom note displayed on desktop or in directories - Antivirus/EDR alert for malware detection - Unexpected system slowness or crashes - Unusual network traffic (C2 beaconing, data exfiltration)

Phase 1: Detection & Initial Response (0-15 minutes)

IMMEDIATE ACTIONS:

1. **Do NOT reboot** infected system (may destroy forensic evidence or trigger additional encryption)
2. **Isolate the infected system:**
   - Physically disconnect network cable, OR
   - Disable network adapter in OS, OR
   - Block MAC address at network switch
   - Leave system powered on (preserves memory forensics)
3. **Alert incident response team:**
   - Call security hotline: [PHONE]
   - Email: security-incident@[COMPANY].com
   - State: “Suspected ransomware on [HOSTNAME], isolated at [TIME]”
4. **Identify scope:**
   - Are multiple systems infected?
   - Check SIEM for alerts on other hosts
   - Check file servers for mass file modification events

Phase 2: Containment & Assessment (15 minutes - 2 hours)

CONTAINMENT ACTIONS:

1. **Disable user accounts** (if user-initiated):
   - Disable compromised user’s AD account
   - Reset password

- Revoke all active sessions (force logoff)

2. **Isolate network segment** (if spreading):
   - If ransomware is actively spreading, isolate VLAN or network segment
   - Block lateral movement at firewall
3. **Preserve evidence:**
   - Take memory dump (if forensic tools available): `FTK Imager`, `Magnet RAM Capture`
   - Screenshot ransom note and encrypted files
   - Export relevant logs (Windows Event Viewer, EDR, SIEM)
   - Document: Date/time discovered, who discovered, initial actions taken

ASSESSMENT QUESTIONS:

- ☐What ransomware variant? (Search ransom note text on Google or ID Ransomware)
- ☐When did encryption start? (Check file modified timestamps)
- ☐How many systems affected?
- ☐Was CUI on affected systems? **If yes, initiate DFARS 72-hour reporting**
- ☐Do we have clean backups? (Check last backup date, verify backup not infected)
- ☐Can we restore from backups? (Estimate recovery time)

Phase 3: Eradication & Recovery (2 hours - days)

ERADICATION ACTIONS:

1. **Identify infection vector:**
   - Phishing email? (Review user's mailbox)
   - Exploited vulnerability? (Check patch status)
   - RDP brute-force? (Review firewall/RDP logs)
2. **Remove malware:**
   - Run antivirus/EDR full scan (if malware still active)
   - If severe: Wipe and reimage infected systems
   - If mild: Use EDR to quarantine and remove malware
3. **Close attack vector:**
   - Patch exploited vulnerability
   - Block malicious IPs/domains at firewall
   - Disable RDP or require VPN access
   - Enhance email filtering (block similar phishing attempts)

RECOVERY ACTIONS:

1. **Restore from backup:**
   - Verify backup is clean (scan backup files for malware before restore)
   - Restore to isolated network segment first (test before production)
   - Validate restored data integrity

2. **Rebuild compromised systems:**
   - Reimage from clean OS media
   - Apply all patches before rejoining network
   - Reinstall applications
   - Restore user data from clean backup
3. **Monitor for reinfection:**
   - Increase SIEM monitoring for 7 days
   - Watch for C2 beaconing or persistence mechanisms
   - Verify malware is fully removed (no remnants)

Phase 4: Post-Incident Activities

LESSONS LEARNED:

- ☐How did ransomware enter environment? (Phishing, RDP, vulnerability?)
- ☐What controls failed? (Email filtering, endpoint protection, user awareness?)
- ☐How can we prevent recurrence? (Patch management, MFA on RDP, security training?)
- ☐Did backups work as expected? (Were they accessible and clean?)
- ☐Document findings in REF-IR-03 Incident Report

RECOMMENDED IMPROVEMENTS:

- Deploy EDR with rollback capability (SentinelOne, CrowdStrike Falcon, Microsoft Defender ATP)
- Implement application whitelisting
- Segment CUI systems from general network
- Test backup restoration monthly (REF-CP-04 Backup Test Log)
- Conduct phishing simulation training (REF-AT-04)

REPORTING:

- ☐Update REF-IR-02 Incident Log with full incident timeline
- ☐If CUI system affected: Submit DFARS 72-hour report to DoD
- ☐Notify cyber insurance provider (if applicable)
- ☐Brief executive leadership on incident and remediation

SCENARIO 2: Phishing / Credential Compromise

Incident Description: User receives phishing email, clicks malicious link, and enters credentials on fake login page. Attacker now has valid username/password.

Detection Indicators: - User reports suspicious email or realizes they entered password on fake site - Unusual login activity (e.g., login from foreign country) - Impossible travel (login from two distant locations within short time) - Email forwarding rule created

(attacker setting up persistence) - Mass emails sent from compromised account (spam/phishing sent to contacts)

Phase 1: Detection & Initial Response (0-10 minutes)

IMMEDIATE ACTIONS:

1. **Disable compromised account:**
   - Azure AD: Disable user account immediately
   - On-premise AD: Disable user account
   - **DO NOT delete account** (preserves logs and mailbox for forensics)
2. **Reset password:**
   - Generate new strong password (16+ characters)
   - Notify user via phone (not email, attacker may have access)
3. **Revoke all sessions:**
   - Azure AD: Revoke refresh tokens (forces re-authentication)
   - O365: Sign out all active sessions
   - VPN: Terminate any active VPN connections for user
4. **Revoke MFA enrollments:**
   - If attacker may have enrolled their own MFA device, revoke all MFA enrollments
   - Require user to re-enroll MFA in-person

Phase 2: Containment & Assessment (10 minutes - 1 hour)

INVESTIGATION ACTIONS:

1. **Review login activity:**
   - Check Azure AD sign-in logs (last 30 days)
   - Identify unauthorized logins (look for unusual IPs, locations, times)
   - Note: Date/time of first unauthorized access
2. **Check email activity:**
   - Review sent items for spam/phishing sent by attacker
   - Check deleted items (attacker may have deleted evidence)
   - Look for email forwarding rules: O365 Admin Center → Users → Mailbox → Mail Flow → Forwarding
   - Check Focused Inbox rules (attackers hide in rules)
3. **Check for persistence mechanisms:**
   - Email forwarding rules (as above)
   - Mailbox delegates (attacker adds themselves as delegate)
   - Application consents (attacker registers OAuth apps with mailbox access)
   - Conditional access bypasses
4. **Assess data access:**
   - What data did user have access to?

- Did attacker access CUI? **If yes, initiate DFARS 72-hour reporting**
- Check OneDrive/SharePoint file activity logs
- Check database access logs (if user has DB access)

Phase 3: Eradication & Recovery (1 hour - 1 day)

ERADICATION ACTIONS:

1. **Remove persistence:**
   - Delete unauthorized email forwarding rules
   - Remove mailbox delegates
   - Revoke suspicious OAuth app consents
   - Review and remove any suspicious Azure AD app registrations
2. **Block attacker access:**
   - Block attacker IP addresses at firewall (if identifiable)
   - Enable geographic restrictions (if attacker from foreign country, block that country)
   - Require MFA re-enrollment (in-person or via video call with manager)
3. **Notify affected parties:**
   - If attacker sent phishing from compromised account, notify recipients
   - Email: "Account was compromised; please disregard recent emails and do not click links"

RECOVERY ACTIONS:

1. **Restore user access:**
   - Re-enable account after password reset and MFA re-enrollment
   - Verify user can log in successfully
   - Confirm no suspicious activity for 24 hours
2. **Monitor for recompromise:**
   - Flag account for enhanced monitoring (7 days)
   - Alert on any unusual login activity
   - Review account activity daily for 1 week

Phase 4: Post-Incident Activities

LESSONS LEARNED:

- ☐How did user fall for phishing? (Convincing email? Lack of training?)
- ☐Why wasn't phishing email blocked? (Email filtering gap?)
- ☐Did MFA prevent attacker access? (If no MFA, is it required now?)
- ☐How quickly did we detect compromise? (Can we improve detection?)

RECOMMENDED IMPROVEMENTS:

- Implement conditional access policies (block legacy auth, require MFA, restrict locations)
- Enable Azure AD Identity Protection (risk-based conditional access)
- Deploy email security (ATP, Proofpoint, Mimecast)
- Conduct phishing simulation training quarterly (REF-AT-04)
- Require MFA for all cloud app access (no exceptions)

REPORTING:

- ☐Update REF-IR-02 Incident Log
- ☐If CUI accessed: Submit DFARS 72-hour report
- ☐Notify user's manager
- ☐Provide security awareness refresher training to user

SCENARIO 3: Unauthorized Access / Privilege Escalation

Incident Description: Attacker gains unauthorized access to system or escalates privileges to administrator/root level.

Detection Indicators: - Unknown user account discovered - User account with unexpected privileges (standard user now admin) - Login from service account (service accounts shouldn't have interactive logins) - Failed sudo/UAC elevation attempts (repeated attempts to gain admin) - Suspicious scheduled tasks or startup items

Phase 1: Detection & Initial Response (0-15 minutes)

IMMEDIATE ACTIONS:

1. **Isolate affected system:**
   - If attacker has current access, isolate network (disconnect or block at firewall)
   - Leave system powered on (forensic evidence)
2. **Disable compromised account:**
   - If unauthorized account created, disable immediately
   - If legitimate account compromised, disable and reset password
3. **Alert incident response team:**
   - Escalate to CISO and security team
   - State: "Unauthorized access detected on [SYSTEM], user [USERNAME]"

Phase 2: Containment & Assessment (15 minutes - 2 hours)

INVESTIGATION ACTIONS:

1. **Identify unauthorized account:**
   - How was account created? (Review security logs: Event ID 4720 on Windows)
   - What privileges does account have?
   - When was it created?

2. **Review access logs:**
   - What did attacker access? (File access logs, database logs)
   - Was CUI accessed? **If yes, initiate DFARS 72-hour reporting**
   - What commands were run? (Check command history: `.bash_history`, PowerShell history)
3. **Check for backdoors:**
   - New scheduled tasks (Windows Task Scheduler, cron jobs)
   - New services or startup items
   - SSH keys added to `~/.ssh/authorized_keys`
   - Webshells on web servers (search for suspicious .php, .asp files)

Phase 3: Eradication & Recovery (2 hours - 1 day)

ERADICATION ACTIONS:

1. **Remove unauthorized access:**
   - Delete unauthorized user accounts
   - Revoke unauthorized privileges from legitimate accounts
   - Remove backdoors (scheduled tasks, services, SSH keys, webshells)
2. **Close vulnerability:**
   - Identify how attacker gained access (exploit? weak password? misconfiguration?)
   - Patch exploited vulnerability
   - Fix misconfiguration (e.g., overly permissive firewall rules)
3. **Reset credentials:**
   - If admin account compromised, reset all admin passwords
   - Rotate service account passwords
   - Consider: Reset all user passwords if domain-wide compromise suspected

RECOVERY ACTIONS:

1. **Rebuild compromised systems** (if root/admin compromise):
   - Wipe and reimage systems with admin-level compromise
   - Attackers may have installed rootkits or kernel-level malware
   - Cannot trust system integrity after root compromise
2. **Restore from clean backup:**
   - If files modified/deleted, restore from backup
   - Verify backup predates compromise
3. **Re-harden systems:**
   - Review privileged account management (implement PAM solution?)
   - Enable audit logging (Windows: Enable audit process creation, Linux: Enable auditd)
   - Implement least privilege (remove unnecessary admin rights)

Phase 4: Post-Incident Activities

LESSONS LEARNED:

- ☐How did attacker gain initial access?
- ☐How did attacker escalate privileges?
- ☐What controls failed? (Vulnerability management? Least privilege?)
- ☐What data was accessed or exfiltrated?

RECOMMENDED IMPROVEMENTS:

- Implement privileged access management (CyberArk, BeyondTrust)
- Deploy EDR with behavior-based detection
- Enable advanced audit logging (command-line logging, process creation)
- Implement Just-In-Time (JIT) admin access (Azure AD PIM)
- Conduct privilege escalation testing (penetration test)

SCENARIO 4: CUI Data Breach / Unauthorized Disclosure

Incident Description: Controlled Unclassified Information (CUI) is accessed, stolen, or disclosed to unauthorized parties.

Detection Indicators: - User reports accidentally emailing CUI to external party - DLP alert: CUI sent outside organization - File server access logs show unusual file downloads - Data found on unauthorized device or location - CUI posted publicly (web, social media, cloud storage)

Phase 1: Detection & Initial Response (0-30 minutes)

IMMEDIATE ACTIONS:

1. **Contain the disclosure:**
   - If email: Attempt message recall (O365 Message Recall, not always successful)
   - If public posting: Contact website/platform to request removal
   - If file share: Remove public access link
   - If cloud storage: Revoke sharing permissions
2. **Initiate DFARS 72-hour reporting:**
   - CUI disclosure/compromise **REQUIRES** DoD reporting within 72 hours
   - Start report clock immediately
3. **Preserve evidence:**
   - Screenshot DLP alert or discovery evidence
   - Save email with CUI attachment (don't delete)
   - Export relevant logs (DLP, email, file access)
4. **Notify CISO and legal counsel:**
   - Potential breach notification obligations (DFARS, state laws, GDPR if EU data)

- Legal counsel advises on notification requirements

Phase 2: Containment & Assessment (30 minutes - 4 hours)

ASSESSMENT ACTIONS:

1. **Identify CUI disclosed:**
   - What specific CUI was involved? (ITAR data, export-controlled, PII, proprietary?)
   - How much data? (Single document, folder, database dump?)
   - Classification level? (CUI Basic, CUI Specified, FOUO?)
2. **Identify unauthorized recipients:**
   - Who received CUI? (Email recipients, link sharers, public?)
   - Are they malicious actors or accidental recipients?
   - Can CUI be retrieved/deleted from recipient?
3. **Determine root cause:**
   - User error (accidental email to wrong person)?
   - System misconfiguration (file share publicly accessible)?
   - Malicious exfiltration (attacker stole data)?
   - Insider threat (employee intentionally disclosed)?
4. **Assess impact:**
   - **Confidentiality impact:** What harm if CUI publicly disclosed?
   - **Compliance impact:** Contract implications, potential CMMC assessment failure
   - **Reputation impact:** Customer trust, media attention

Phase 3: Eradication & Recovery (4 hours - days)

CONTAINMENT ACTIONS:

1. **Request recipient deletion:**
   - If accidental disclosure, contact recipient and request deletion (document request)
   - Verify deletion (if possible, get written confirmation)
   - If malicious actor, assume data is retained
2. **Remove public postings:**
   - Submit takedown request to website/platform
   - If cloud storage, disable share links and download access
3. **Fix disclosure vector:**
   - User error: Provide remedial training
   - System misconfiguration: Fix configuration (remove public access)
   - Malicious exfiltration: Investigate and remove attacker access (see Scenario 3)
   - Insider threat: Involve HR and legal (potential termination)

RECOVERY ACTIONS:

1. **Notify affected parties:**
   - **DoD Contracting Officer:** DFARS 72-hour report (required)
   - **Customers:** If their data disclosed (contractual obligation)
   - **Individuals:** If PII disclosed (state breach notification laws)
   - **Insurance provider:** If cyber insurance covers breach response
2. **Provide breach response services** (if PII involved):
   - Credit monitoring for affected individuals
   - Identity theft protection
   - Notification letter with instructions
3. **Enhance DLP controls:**
   - Implement DLP policy to prevent future disclosures
   - Block external email attachments with CUI keywords
   - Require encryption for external email with sensitive data

Phase 4: Post-Incident Activities

LESSONS LEARNED:

- ☐How was CUI disclosed? (User error, misconfiguration, malicious?)
- ☐Why didn't DLP prevent disclosure?
- ☐What controls failed? (User training, technical controls, process?)
- ☐What changes needed to prevent recurrence?

RECOMMENDED IMPROVEMENTS:

- Implement Microsoft Information Protection (AIP labels)
- Enable DLP policies (O365 DLP, network DLP, endpoint DLP)
- Conduct CUI handling training (REF-AT-03)
- Implement CUI boundary controls (network segmentation)
- Enhance email controls (external email banner, block CUI to external)

REPORTING:

- ☐DFARS 72-hour report to DoD (**REQUIRED**)
- ☐Update REF-IR-02 Incident Log
- ☐Breach notification (if PII) per state laws
- ☐Notify customer per contract terms
- ☐Document in REF-IR-03 Incident Report Template

SCENARIO 5: Lost or Stolen Device with CUI

Incident Description: Laptop, tablet, phone, USB drive, or external hard drive containing CUI is lost or stolen.

Detection Indicators: - User reports lost/stolen device - Device fails to check in with MDM (Mobile Device Management) - Device location services show device in unusual location

Phase 1: Detection & Initial Response (0-15 minutes)

IMMEDIATE ACTIONS:

1. **Gather device information:**
   - Device type (laptop, phone, tablet, USB)
   - Asset tag / serial number
   - Last known location
   - CUI stored on device? If yes, what specific CUI?
2. **Remote wipe device** (if MDM enrolled):
   - Microsoft Intune: Issue remote wipe command
   - Apple iCloud: Use Find My iPhone → Erase Device
   - Android: Use Find My Device → Erase Device
   - BitLocker: Issue BitLocker recovery key and remote wipe
3. **Disable user account** (if device compromised):
   - Disable AD account to prevent device from accessing network resources
   - Reset user password
4. **Initiate DFARS 72-hour reporting** (if CUI on device):
   - Assume CUI compromised if device not encrypted or cannot be confirmed wiped

Phase 2: Containment & Assessment (15 minutes - 2 hours)

ASSESSMENT ACTIONS:

1. **Determine CUI risk:**
   - Was device encrypted? (BitLocker, FileVault, device encryption)
   - Was CUI actually on device? (Check file inventory, user confirmation)
   - Can device be located? (GPS, MDM location services)
   - Is device password/PIN protected?
2. **Determine incident classification:**
   - **Low Risk:** Device encrypted + strong password + remote wipe successful
   - **Medium Risk:** Device encrypted + weak password OR remote wipe unconfirmed
   - **High Risk:** Device not encrypted OR CUI confirmed on device
3. **Attempt device recovery:**
   - If lost (not stolen), contact lost & found, retrace steps
   - If stolen, consider police report (especially if high-value CUI)

Phase 3: Eradication & Recovery (2 hours - days)

CONTAINMENT ACTIONS:

1. **Change credentials:**
   - Reset passwords for all accounts accessible from device
   - Revoke MFA enrollments (if MFA app on lost device)
   - Rotate VPN client certificates
2. **Block device network access:**
   - Block device by MAC address at network edge
   - Remove device from MDM (if unrecoverable)
   - Revoke device certificates
3. **Monitor for unauthorized access:**
   - Watch for login attempts from lost device (IP address, device ID)
   - Alert on any successful authentications from device

RECOVERY ACTIONS:

1. **Issue replacement device:**
   - Provision new laptop/phone from IT inventory
   - Enroll in MDM before issuing to user
   - Restore user data from backup (if available)
2. **Notify affected parties:**
   - If CUI on device: DFARS 72-hour report to DoD
   - If PII on device: Breach notification per state laws (if encryption not confirmed)
   - Customer notification (if contractually required)

Phase 4: Post-Incident Activities

LESSONS LEARNED:

- ☐Was device encrypted? (If no, why not?)
- ☐Was remote wipe successful? (If no, why not? Not MDM-enrolled?)
- ☐Did user follow physical security policy? (Device left in car, coffee shop?)
- ☐What controls prevent future incidents?

RECOMMENDED IMPROVEMENTS:

- Enforce full-disk encryption (BitLocker, FileVault) via Group Policy/MDM
- Require MDM enrollment for all CUI devices
- Prohibit CUI on removable media (USB drives) unless encrypted
- Conduct physical security training (don't leave devices unattended)
- Implement endpoint DLP (prevent CUI from being copied to removable media)

REPORTING:

- ☐DFARS 72-hour report (if CUI compromised or cannot confirm device wiped/encrypted)
- ☐Update REF-IR-02 Incident Log

- ☐Police report (if high-value or theft suspected)
- ☐Insurance claim (if applicable)

Additional Quick-Reference Scenarios

SCENARIO 6: Denial of Service (DoS/DDoS) Attack

Immediate Actions: 1. Confirm attack (vs. legitimate traffic spike) 2. Contact ISP to enable DDoS mitigation (if available) 3. Block attacking IP addresses at firewall (if small-scale) 4. Enable rate limiting / connection throttling 5. Activate DDoS protection service (Cloudflare, Akamai) 6. Document attack characteristics (IPs, traffic volume, target)

Recovery: - Restore services once attack subsides - Implement DDoS protection for future prevention - No DFARS reporting unless CUI systems unavailable > 24 hours

SCENARIO 7: Insider Threat

Immediate Actions: 1. Coordinate with HR and legal (before taking IT actions) 2. Preserve evidence (do NOT alert insider) 3. Monitor insider's activity (email, file access, logins) 4. When ready: Disable accounts, revoke access, escort from premises 5. Image devices and review activity logs 6. If CUI exfiltrated: Initiate DFARS 72-hour report

Key Consideration: Legal and HR involvement critical; follow company HR policy and consult legal counsel before acting.

SCENARIO 8: Vendor/Supply Chain Breach

Immediate Actions: 1. Contact vendor to confirm breach and scope 2. Assess: Does vendor have access to our systems/data? 3. Disable vendor access (VPN, API keys, passwords) until cleared 4. Review vendor access logs (what did they access?) 5. If CUI vendor-accessible: Initiate DFARS 72-hour report 6. Request vendor's breach notification and incident report

Recovery: - Review vendor security posture (REF-TP-03 Vendor Assessment) - Consider replacing vendor if security inadequate - Enhance vendor access controls (least privilege, MFA, logging)

---

4. EVIDENCE COLLECTION & PRESERVATION

4.1 Types of Evidence

4.2 Evidence Handling Procedures

Chain of Custody: 1. Document who collected evidence, when, and from where 2. Store evidence in secure location (encrypted storage, access-controlled folder) 3. Maintain log of who accessed evidence and when 4. Use write-blocker when imaging disks (prevents modification)

Evidence Folder Structure:

```
/Incident-YYYY-MM-DD-[Brief-Description]/
├── 00-Incident-Summary.txt (Timeline, systems involved, actions taken)
├── 01-Network-Logs/
│   ├── firewall-logs-YYYY-MM-DD.csv
│   └── SIEM-alerts-YYYY-MM-DD.pdf
├── 02-System-Logs/
│   ├── EventViewer-Security-Export.evtx
│   └── syslog-export.log
├── 03-Email-Evidence/
│   ├── phishing-email.eml
│   └── message-headers.txt
├── 04-File-System/
│   ├── ransomware-note.txt
│   └── malware-sample.bin (password-protected .zip)
├── 05-Screenshots/
│   ├── screenshot-ransom-note.png
│   └── screenshot-DLP-alert.png
└── 06-Reports/
    └── REF-IR-03-Incident-Report.md
```

---

5. POST-INCIDENT ACTIVITIES

5.1 Incident Report (REF-IR-03)

After every incident, complete REF-IR-03 Incident Report Template with: - Incident timeline - Root cause analysis - Impact assessment - Actions taken - Lessons learned - Recommendations

5.2 Lessons Learned Meeting

When: Within 1 week of incident closure

Attendees: - Incident Commander - Incident response team members - System owners - Management (if critical incident)

Agenda: 1. Review incident timeline 2. Discuss what went well 3. Discuss what could be improved 4. Identify process improvements 5. Assign action items (update playbook, implement new control, etc.)

5.3 Continuous Improvement

Action Items: - Update this playbook with new scenarios or improved procedures - Update detection rules in SIEM - Enhance technical controls (DLP, EDR, firewall rules) - Conduct tabletop exercises (test incident response) - Provide additional training (user awareness, technical skills)

---

6. C3PAO ASSESSMENT GUIDANCE

What C3PAOs Look For

1. **Documented Incident Response Procedures**
   - Written playbook available to incident responders
   - Procedures tested and validated
2. **DFARS 72-Hour Reporting Process**
   - Clear understanding of when DoD reporting required
   - Process documented and communicated to team
3. **Evidence of Incident Handling**
   - Incident logs showing real incidents handled
   - Documentation of response actions taken
   - Lessons learned documented
4. **Regular Testing**
   - Tabletop exercises conducted annually
   - Incident response plan tested

Evidence to Provide C3PAO

Sample C3PAO Interview Questions

Q1: "Walk me through your incident response process."

Good Answer: "We follow the NIST SP 800-61 incident response lifecycle documented in our playbook (REF-IR-01). When an incident is detected—via SIEM alert, user report, or EDR detection—our on-call security analyst triages the incident and determines severity. For high or critical incidents, we immediately notify the CISO and assemble our incident response team. We use scenario-specific playbooks for common incidents like ransomware, phishing, or data breaches. Each playbook has step-by-step procedures for containment, eradication, and recovery. Every incident is logged in REF-IR-02 Incident Log, and we complete an incident report (REF-IR-03) afterward with lessons learned. We conduct a lessons learned meeting within one week of closing critical incidents to identify improvements."

Q2: "How do you handle DFARS 72-hour reporting for CUI incidents?"

Good Answer: "Any cyber incident that affects CUI or systems processing CUI requires reporting to DoD within 72 hours per DFARS 252.204-7012. Our playbook clearly defines when reporting is required—examples include malware on a CUI system, unauthorized CUI access, or potential CUI exfiltration. The 72-hour clock starts when we discover the incident, not when it occurred. Our CISO is responsible for submitting reports via the DoD DC3 portal at dibnet.dod.mil. We document all DoD reporting in our incident log (REF-IR-02) and include the report confirmation number. We also preserve forensic evidence in case DoD requests media or further investigation. We've conducted tabletop exercises specifically on CUI incident scenarios to ensure our team understands the reporting requirements."

Q3: "Show me an example of an incident you've responded to."

Good Answer: "Here's an incident from June 2024 (REF-IR-02, incident INC-2024-042). A user reported their laptop missing after business travel. The device had CUI access, so we immediately initiated our Lost/Stolen Device playbook (REF-IR-01, Scenario 5). We issued a remote wipe via Intune, disabled the user's account, and reset their password. The device was BitLocker-encrypted, so even if the wipe failed, CUI was protected. We verified the wipe succeeded via Intune console. Because we confirmed the device was encrypted and wiped, we determined no CUI compromise occurred, so DFARS reporting was not required. We still documented the incident thoroughly, issued a replacement device, and reminded the user about physical security policy. Here's the full incident report (REF-IR-03) with timeline, actions taken, and lessons learned."

---

7. REVISION HISTORY

Version	Date	Author	Changes
1.0	[Initial Date]	[CISO Name]	Initial creation of incident response playbook
2.0	[Current Date]	Keystone Command	Comprehensive expansion with 8 detailed scenarios, DFARS 72-hour reporting, evidence collection, C3PAO guidance, post-incident procedures

---

DOCUMENT CONTROL

Classification: CUI (contains security procedures and contact information) **Retention Period:** 7 years after superseded **Review Frequency:** Annual (or after major incident) **Distribution:** CISO, Incident Response Team, IT Staff, Security Team

---

END OF DOCUMENT

This playbook is part of the Keystone Command CMMC Level 2 Complete Documentation Package. Customize contact information, system names, and procedures to match your organization.