DOMINUS GRAY, LLC

Securing Access to Opportunity

Incident Response Plan

NIST SP 800-171 / DFARS 252.204-7012 / CMMC Level 2

PREPARED FOR

Meridian Defense Systems, Inc.

February 2026

Document ID: DG-IRP-2026-001

CONFIDENTIAL — DO NOT DISTRIBUTE

SDVOSB | MBE | NaBOVA | VetHUB | SAM.gov Registered

Service-Disabled Veteran-Owned Small Business

Table of Contents

1. Document Control

Version History

VERSION	DATE	AUTHOR	CHANGES
1.0	02/09/2026	Dominus Gray, LLC	Initial release — full IRP baseline
0.2	01/28/2026	Dominus Gray, LLC	Incorporated client review feedback
0.1	01/13/2026	Dominus Gray, LLC	Draft for internal review

Distribution List

NAME	ROLE / TITLE	COPY TYPE	DATE ISSUED
[Executive Sponsor]	VP of Information Security	Controlled	02/09/2026
[IR Manager]	Incident Response Manager	Controlled	02/09/2026
[Lead Analyst]	Senior Security Analyst	Controlled	02/09/2026
[IT Director]	Director of IT Operations	Controlled	02/09/2026
[General Counsel]	Legal Counsel	Controlled	02/09/2026
[Contracts Manager]	DoD Contracts Manager	Controlled	02/09/2026

Review Schedule

This Incident Response Plan shall be reviewed and updated under the following

conditions:

- Annually — Full review and update no later than February of each calendar year
- After every SEV-1 or SEV-2 incident — Within 30 days of post-incident review completion
- Upon significant infrastructure changes — Network architecture, CUI boundary, or tooling changes
- Upon changes to DFARS/CMMC requirements — Within 60 days of published regulatory updates
- After organizational changes — Changes to CSIRT membership, leadership, or contact information

2. Purpose and Scope

Purpose

This Incident Response Plan (IRP) establishes a structured, repeatable framework for Meridian Defense Systems, Inc. to prepare for, detect, analyze, contain, eradicate, and recover from cybersecurity incidents affecting the organization's information systems, networks, and data — with specific emphasis on the protection of Controlled Unclassified Information (CUI) in accordance with Department of Defense (DoD) requirements.

This plan satisfies the following compliance requirements:

- NIST SP 800-171 Rev 2 — IR.L2-3.6.1 (Incident Handling), IR.L2-3.6.2 (Incident Reporting), IR.L2-3.6.3 (Incident Response Testing)
- DFARS 252.204-7012 — Safeguarding Covered Defense Information and Cyber Incident Reporting
- CMMC Level 2 — Incident Response (IR) domain requirements

Scope

This plan applies to:

- All information systems, networks, and applications within the CUI security boundary
- All personnel with access to CUI or CUI-processing systems (employees, contractors, subcontractors)
- All Meridian Defense Systems, Inc. facilities processing, storing, or transmitting CUI (3 locations)
- Cloud services and external systems within the CUI data flow (Microsoft 365 GCC High, Azure Government)

- Third-party service providers with access to the CUI environment

> **NIST SP 800-171 — IR.L2-3.6.1: Incident Handling**
>
> "Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities."

Out of Scope: Personal devices not connected to the corporate network, public-facing marketing website (non-CUI), and physical security incidents without a cyber component (handled under separate Physical Security Plan).

3. Incident Response Team (CSIRT)

The Meridian Defense Systems, Inc. Computer Security Incident Response Team (CSIRT) is responsible for executing this plan. The CSIRT operates under the authority of the Executive Sponsor and is led by the IR Manager. All CSIRT members must complete annual incident response training and participate in tabletop exercises.

ROLE	PRIMARY RESPONSIBILITIES	CONTACT
IR Manager	Overall incident command; coordinates response activities; authorizes containment actions; manages DFARS reporting timeline	[Name] [Phone] [Email]
Lead Analyst	Technical investigation lead; evidence collection and analysis; malware analysis; forensic imaging; IOC identification	[Name] [Phone] [Email]
Communications Lead	Internal/external communications; stakeholder notifications; media coordination; DoD contracting officer liaison	[Name] [Phone] [Email]
Legal Counsel	Legal review of incident response; regulatory compliance; evidence preservation guidance; breach notification obligations	[Name] [Phone] [Email]
IT Operations	System isolation and containment; network segmentation; backup/restore operations; system rebuilds; monitoring	[Name] [Phone] [Email]

ROLE	PRIMARY RESPONSIBILITIES	CONTACT
Executive Sponsor	Strategic decision authority; resource allocation; business impact decisions; board/executive communication; DoD relationship management	[Name] [Phone] [Email]

Activation Criteria

The CSIRT is activated when any of the following occur:

- A potential or confirmed security incident is reported involving CUI systems
- An intrusion detection/prevention system generates a high-severity alert
- A third party (DC3, FBI, vendor) notifies the organization of a potential compromise
- Anomalous activity is detected on CUI boundary systems
- A CUI spillage event is identified

4. Incident Classification

All security events and incidents shall be classified using the following severity matrix. Classification determines response urgency, escalation requirements, resource allocation, and DoD reporting obligations.

SEV-1 — CRITICAL

DEFINITION
Active compromise of CUI systems; data exfiltration confirmed or imminent; complete loss of critical business operations; active APT/nation-state threat actor.

EXAMPLES
Ransomware on CUI servers, confirmed CUI exfiltration, active command-and-control traffic from CUI enclave, domain controller compromise.

RESPONSE SLA
15 minutes initial response; CSIRT full activation within 1 hour; 24/7 operations until resolved.

ESCALATION
Immediate: IR Manager, Executive Sponsor, Legal Counsel. Within 1 hour: DoD contracting officer, DC3 (initiate 72-hr reporting clock).

SEV-2 — HIGH

DEFINITION
Confirmed unauthorized access to CUI environment; malware detected on CUI systems; significant service disruption; CUI spillage to unauthorized systems.

EXAMPLES
Malware on CUI endpoint, unauthorized access to CUI file share, CUI found on unencrypted device, phishing compromise of CUI-privileged account.

RESPONSE SLA
30 minutes initial response; CSIRT activation within 2 hours; extended hours as needed.

ESCALATION
Within 30 min: IR Manager, Lead Analyst. Within 2 hours: Executive Sponsor, Legal Counsel. Evaluate DFARS reporting requirement.

SEV-3 — MEDIUM

DEFINITION
Suspicious activity on CUI boundary; policy violations involving CUI access; attempted but unsuccessful intrusion; non-CUI system compromise with potential CUI impact.

EXAMPLES
Failed brute-force against CUI VPN, policy violation by CUI-authorized user, vulnerability exploited on non-CUI system adjacent to CUI boundary.

RESPONSE SLA
2 hours initial response; investigation within 1 business day.

ESCALATION
Within 2 hours: IR Manager. Within 4 hours: Lead Analyst. Executive Sponsor notified at next business day if no escalation.

SEV-4 — LOW

DEFINITION
Security events with minimal impact; routine policy violations; scanning/reconnaissance activity; non-CUI system incidents with no CUI boundary impact.

EXAMPLES
Port scanning from external IP, single failed login attempt, low-risk vulnerability identified, spam/phishing with no click-through.

RESPONSE SLA
1 business day initial response; resolution within 5 business days.

ESCALATION
IR Manager notified via daily summary. No immediate escalation unless pattern detected.

5. Incident Response Phases

This plan follows the NIST SP 800-61 Rev 2 incident response lifecycle. Each phase includes specific procedures, responsibilities, and deliverables tailored to CUI protection requirements.

NIST Incident Response Lifecycle

Preparation → Detection & Analysis → Containment → Eradication → Recovery → Post-Incident Activity

The lifecycle is iterative — findings during any phase may require returning to a previous phase.

5.1 Preparation

The Preparation phase establishes the foundation for effective incident response. This includes maintaining tools, training personnel, and ensuring communication readiness.

NIST CSF 2.0 Alignment

This IRP aligns with NIST Cybersecurity Framework 2.0 (February 2024), which adds a new Govern function emphasizing organizational context and risk management strategy. The six IR phases map to CSF 2.0 Respond (RS) and Recover (RC) functions.

Monitoring & Detection Tools

- SIEM Platform — Centralized log aggregation, correlation, and alerting (e.g., Splunk, Microsoft Sentinel)
- EDR Solution — Endpoint detection and response on all CUI endpoints and servers
- Network IDS/IPS — Deployed at CUI boundary and key network segments
- Vulnerability Scanner — Monthly authenticated scans of all CUI-boundary systems
- Email Security Gateway — Advanced threat protection with sandboxing for CUI-authorized users
- DLP Solution — Data Loss Prevention monitoring on CUI egress points
- Firewall & Network Monitoring — Next-gen firewall with logging at CUI boundary

Training Requirements

- Annual incident response training for all CSIRT members (IR.L2-3.6.3)
- Tabletop exercises — Minimum twice annually, including one CUI-specific scenario
- Technical training — Forensic analysis, malware reverse engineering for Lead Analyst
- CUI awareness training — All personnel with CUI access, annually
- DFARS reporting procedures — Annual training for IR Manager and Communications Lead

Communication Readiness

- Maintain current contact roster for all CSIRT members (primary + backup)
- Out-of-band communication channel (encrypted messaging app, satellite phone)
- Pre-drafted communication templates for stakeholder notification (see Section 8)
- DC3/DCISE portal account credentials maintained and tested quarterly
- Incident response "go bag" — forensic laptops, write blockers, storage media, documentation kits

Continuous Monitoring Requirements

Implement continuous monitoring per NIST SP 800-137 to detect incidents proactively rather than reactively. Key capabilities include:

- Automated vulnerability scanning (monthly minimum)
- SIEM/SOAR integration for real-time alerting
- Endpoint detection and response (EDR) on all CUI systems
- Network traffic analysis at CUI boundary points
- User behavior analytics (UBA) for insider threat detection

5.2 Detection & Analysis

Timely detection and accurate analysis are critical to minimizing the impact of security incidents on CUI systems.

Indicators of Compromise (IOC) Categories

- Network-based — Unusual outbound traffic from CUI enclave, connections to known-bad IPs/domains, DNS anomalies, unexpected encrypted traffic
- Host-based — Unexpected processes, registry changes, new services, file integrity changes on CUI servers, anti-malware alerts
- Account-based — Failed login patterns, privilege escalation, off-hours access to CUI systems, impossible travel (geographic anomaly)
- Data-based — Unusual data transfers, large file copies from CUI shares, email with CUI markers to external recipients, USB activity on CUI endpoints

- Application-based — Web application attacks, SQL injection attempts, API abuse, unexpected application behavior on CUI-processing applications

Analysis Procedures

- Triage — Validate alert, determine if event is a true positive, assign initial severity classification
- Scope Assessment — Identify affected systems, data types (CUI vs. non-CUI), network segments, and user accounts
- Timeline Construction — Establish initial, current, and projected scope of incident using log data
- Impact Analysis — Determine business impact, CUI exposure, and potential DFARS reporting obligation
- Attribution (if possible) — Identify threat actor TTPs using MITRE ATT&CK framework mapping

> **Evidence Preservation — Critical First Step**
>
> Before ANY remediation or containment action, ensure volatile evidence is captured:
> • Memory dumps of affected systems
> • Running process lists and network connections
> • System and security event logs
> • Screenshots of anomalous activity
> See Section 9 (Evidence Handling) for detailed procedures.

5.3 Containment

Containment limits the damage of an incident and prevents further compromise. Strategies are divided into short-term (immediate) and long-term (sustained) actions.

Short-Term Containment (Immediate — Hours)

- Network isolation of affected CUI systems (VLAN reassignment, firewall rule changes)
- Disable compromised user accounts and revoke active sessions
- Block identified malicious IPs, domains, and hashes at perimeter and endpoint
- Quarantine affected endpoints via EDR solution
- Redirect DNS for compromised systems to sinkhole
- Preserve system state — do NOT reboot or rebuild until forensic image is captured

Long-Term Containment (Sustained — Days)

- Deploy additional monitoring on CUI boundary segments
- Implement temporary network segmentation to further isolate CUI enclave
- Rebuild compromised systems on clean media (maintain originals for forensics)
- Reset credentials for all accounts with access to affected systems
- Engage third-party forensic support if scope exceeds internal capability

Containment Decision Matrix

DECISION FACTOR	ISOLATE IMMEDIATELY	MONITOR & CONTAIN
CUI Data at Risk	CUI confirmed exposed	CUI not yet accessed
Active Exfiltration	Data leaving network	No outbound data flow
Lateral Movement	Spreading to other systems	Isolated to single host
Business Impact	Critical ops affected	Non-critical systems only
Threat Actor	APT/nation-state indicators	Opportunistic/automated

5.4 Eradication

Eradication removes the root cause of the incident and eliminates all traces of the threat actor from the environment.

Root Cause Removal

- Identify and remove all malware, backdoors, rootkits, and unauthorized tools
- Patch or mitigate the vulnerability exploited for initial access
- Remove unauthorized user accounts, services, and scheduled tasks
- Clean or rebuild affected systems from known-good baselines
- Verify eradication across all affected systems — re-scan with updated IOCs

System Hardening

- Apply all pending security patches to CUI-boundary systems
- Review and tighten firewall rules based on incident findings
- Update EDR/AV signatures and detection rules with incident-specific IOCs
- Rotate all credentials (passwords, API keys, certificates) for affected systems
- Review and restrict permissions — enforce least privilege based on lessons learned

- Update SIEM correlation rules and alerts based on attack patterns observed

5.5 Recovery

Recovery restores affected systems and services to normal operation while maintaining heightened vigilance.

Restoration Procedures

- Restore systems from verified clean backups — validate backup integrity before restoration
- Rebuild systems from hardened baselines where backups may be compromised
- Reconnect systems to network in staged approach — CUI systems last
- Re-enable user accounts with new credentials; require MFA re-enrollment
- Restore data from backup with integrity verification (hash comparison)

Validation Testing

- Vulnerability scan of all restored systems — confirm no residual vulnerabilities
- Verify CUI boundary controls are restored and functioning (firewall, IDS/IPS, DLP)
- Confirm SIEM is collecting logs from all restored systems
- Business function testing — verify restored systems support required operations
- User acceptance testing — confirm CUI access and workflow functionality

Enhanced Monitoring

- Increase monitoring sensitivity on restored systems for 30 days minimum
- Deploy additional logging on previously compromised systems
- Monitor for recurrence using incident-specific IOCs
- Daily review of SIEM alerts for restored CUI systems during monitoring period
- Weekly status reports to Executive Sponsor during recovery monitoring phase

5.6 Post-Incident Activity

Post-incident activities capture lessons learned and drive continuous improvement of the incident response capability.

Lessons Learned Meeting

- Conduct within 5 business days of incident closure for SEV-1/SEV-2; 10 days for SEV-3
- All CSIRT members and relevant stakeholders must attend
- Review: What happened? When was it detected? How effective was the response?
- Identify gaps in tools, processes, training, or communication
- Document action items with owners and deadlines

Post-Incident Report Template

- Executive Summary — Incident overview, impact, and resolution
- Incident Timeline — Complete chronology from detection to closure
- Root Cause Analysis — How the incident occurred and contributing factors
- Impact Assessment — Systems affected, data exposed, business disruption, CUI impact
- Response Effectiveness — What worked, what did not, response time analysis
- Recommendations — Specific improvements to prevent recurrence
- Compliance Actions — DFARS reporting status, evidence preservation status

Process Improvement

- Update this IRP based on lessons learned — document changes in Version History
- Update detection rules and SIEM content based on incident patterns
- Revise training materials to incorporate lessons learned
- Update tabletop exercise scenarios based on real incident experience
- Brief executive leadership on incident trends and resource requirements
- IR.L2-3.6.3: Test updated incident response capability within 90 days of plan revision

6. CUI-Specific Procedures

The following procedures address incident types unique to organizations handling Controlled Unclassified Information under DoD contracts.

6.1 CUI Spillage Handling

A CUI spillage occurs when CUI is transferred to an information system or media that is not authorized to process, store, or transmit CUI.

Spillage Response Procedure

- IDENTIFY — Determine the scope of CUI data involved and the unauthorized system(s) affected
- ISOLATE — Disconnect the unauthorized system from the network to prevent further spread
- NOTIFY — Inform the IR Manager immediately; classify as minimum SEV-2
- PRESERVE — Do not delete the spilled CUI; preserve for forensic review and evidence
- CONTAIN — Identify all copies, caches, backups, and replicas of the spilled data
- SANITIZE — After forensic preservation, securely wipe CUI from unauthorized systems using NIST SP 800-88 procedures

- VERIFY — Confirm sanitization is complete; obtain written confirmation from system owner
- REPORT — Document the spillage in the incident tracking system; evaluate DFARS reporting obligation
- REMEDIATE — Implement controls to prevent recurrence (DLP rules, access controls, training)

6.2 CUI Boundary Breach Procedures

A CUI boundary breach occurs when an unauthorized entity gains access to the CUI enclave or when CUI data flows outside the defined security boundary.

CUI Boundary Breach — Automatic SEV-1 Classification

Any confirmed breach of the CUI security boundary is automatically classified as SEV-1 and triggers:
- Full CSIRT activation within 1 hour
- DFARS 72-hour reporting clock initiation
- Contracting Officer notification
- Legal Counsel engagement
- Forensic imaging of boundary systems

- Immediately isolate the breached network segment at the firewall/switch level
- Capture forensic images of CUI boundary devices (firewalls, jump servers, DMZ hosts)
- Review all CUI data flows for unauthorized egress — DLP logs, firewall logs, proxy logs
- Identify all CUI data potentially exposed — by type, classification, contract, and volume
- Assess whether covered defense information (CDI) was compromised — triggers DFARS reporting
- Engage third-party forensic firm if APT/nation-state actor suspected
- Maintain 90-day image preservation per DFARS requirements

6.3 Export-Controlled Information Considerations

If the organization handles ITAR (International Traffic in Arms Regulations) or EAR (Export Administration Regulations) controlled data alongside CUI, additional incident response obligations apply:

- Report to the Directorate of Defense Trade Controls (DDTC) for ITAR data exposure
- Report to the Bureau of Industry and Security (BIS) for EAR data exposure
- Restrict incident response team access to U.S. persons only for ITAR incidents

- Document export classification of all affected data in the incident report

7. DoD Reporting Requirements

DFARS 252.204-7012 — Cyber Incident Reporting

"When the Contractor discovers a cyber incident that affects a covered contractor information system or the covered defense information residing therein, or that affects the contractor's ability to perform the requirements of the contract that are designated as operationally critical support and identified in the contract, the Contractor shall — (A) Conduct a review of the evidence of the cyber incident and preserve images of all known affected information systems and all relevant monitoring/packet capture data for at least 90 days; (B) Rapidly report the cyber incident to the DoD within 72 hours."

⚠ FALSE CLAIMS ACT LIABILITY

Failure to report cyber incidents within 72 hours, or failure to preserve forensic images for 90 days, may constitute grounds for False Claims Act enforcement under the DOJ Civil Cyber-Fraud Initiative. A February 2025 settlement of $11.3M demonstrates active DOJ enforcement of cybersecurity compliance obligations.

DCISE Portal Reporting Workflow

Note: The legacy DIBNet portal was decommissioned on June 6, 2025. All cyber incident reports must now be submitted through the DCISE portal. The new workflow is: submit incident details into ICF portal (https://icf.dcise.cert.org) → system generates .xml file → submit .xml to DC3 via encrypted email or DoD SAFE.

7.1 What Constitutes a "Cyber Incident" Under DFARS

A "cyber incident" is defined as actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein. Specifically:

- Unauthorized access to a covered contractor information system
- Any compromise of covered defense information (CDI) residing on contractor systems
- Any event that adversely affects the contractor's ability to perform operationally critical support
- Exfiltration, manipulation, or destruction of CUI/CDI by a threat actor
- Ransomware or destructive malware affecting systems processing CUI/CDI

7.2 72-Hour Reporting Timeline

The 72-hour clock begins when the contractor discovers the cyber incident — NOT when analysis is complete. The following timeline governs DoD reporting:

TIMEFRAME	REQUIRED ACTION	RESPONSIBLE PARTY
T+0	Incident discovered — 72-hour clock begins	Discovering party / SOC
T+1 hour	IR Manager notified; initial classification	IR Manager
T+4 hours	CSIRT activated; evidence preservation initiated	IR Manager / Lead Analyst
T+12 hours	Initial scope assessment complete	Lead Analyst
T+24 hours	DFARS reporting determination made	IR Manager / Legal Counsel
T+48 hours	Draft DCISE portal submission prepared and reviewed	IR Manager / Comms Lead
T+72 hours	Report submitted to DC3 via DCISE portal (ICF)	IR Manager
T+72 hours	Contracting Officer notified	Communications Lead

7.3 Required Information for DoD Reporting

The DCISE portal (ICF) submission must include the following information (to the extent known at time of reporting):

- Company name, CAGE code, and contract number(s) affected
- Date the incident was discovered and date the incident occurred (if known)
- Type of compromise (unauthorized access, exfiltration, malware, etc.)
- Description of the technique or method used by the threat actor
- Affected programs, contracts, and types of CUI/CDI involved

- Number and type of systems affected
- Indicators of compromise (IP addresses, domains, file hashes, malware samples)
- Impact assessment — what data was potentially accessed or exfiltrated
- Actions taken to contain and remediate the incident
- Point of contact for DoD follow-up (name, phone, email, clearance level)

7.4 Image Preservation Requirements

90-Day Image Preservation Requirement

DFARS requires preservation of forensic images of all known affected information systems and all relevant monitoring/packet capture data for a minimum of 90 days from the date of the report to DC3. This data must be:

• Stored securely with documented chain of custody
• Available for DoD damage assessment activities (DC3 may request media and additional information)
• Maintained on write-protected or write-once media
• Accessible to authorized government personnel upon request

Failure to preserve images may result in contract penalties and False Claims Act liability.

7.5 Contracting Officer Notification

In addition to the DC3/DCISE portal report, the following notifications are required:

- Notify the Contracting Officer (CO) of the cyber incident within 72 hours
- Provide the CO with the DCISE portal incident report number
- If subcontractor systems are affected, notify the prime contractor immediately
- If the organization IS a subcontractor, notify the prime contractor who will report to DC3
- Provide updates to the CO as additional information becomes available during investigation

8. Communication Plan

8.1 Internal Notification Matrix

The following matrix defines who is notified, when, and by whom for each severity level:

STAKEHOLDER	SEV-1	SEV-2	SEV-3	SEV-4
IR Manager	Immediate	< 30 min	< 2 hours	Daily summary
Lead Analyst	Immediate	< 2 hours	< 4 hours	As needed
Executive Sponsor	< 1 hour	< 4 hours	Next business day	Monthly report
Legal Counsel	< 1 hour	< 4 hours	As needed	Not required
IT Operations	Immediate	< 1 hour	< 4 hours	As needed
Comms Lead	< 1 hour	< 2 hours	As needed	Not required
All Staff	As directed	As directed	Not required	Not required

8.2 External Communication

DoD / Government Agencies

- DC3 (Defense Cyber Crime Center) — DCISE portal submission via ICF (Incident Collection Format) within 72 hours of discovery
- Contracting Officer — Notification within 72 hours; provide DCISE portal incident report number
- CISA (Cybersecurity & Infrastructure Security Agency) — Optional but recommended for significant incidents
- FBI Cyber Division — If criminal activity suspected or APT/nation-state actor identified

Media Communication

- All media inquiries directed to Communications Lead — no other personnel may speak to media
- Media statements must be approved by Executive Sponsor and Legal Counsel before release

- Do NOT disclose CUI classification, specific systems, contract details, or technical IOCs to media
- Coordinate with DoD Public Affairs if incident involves classified or sensitive programs

8.3 Stakeholder Communication Templates

Pre-approved communication templates are maintained for the following scenarios:

- Template 1: Initial internal notification to CSIRT members
- Template 2: Executive briefing (verbal and written formats)
- Template 3: Contracting Officer notification letter
- Template 4: Employee notification (general — no technical details)
- Template 5: Customer/partner notification (if contractually required)
- Template 6: Regulatory notification (state breach notification laws, if applicable)

9. Evidence Handling

Proper evidence handling is critical for forensic analysis, regulatory compliance (DFARS 90-day preservation), and potential legal proceedings. All evidence handling must maintain chain of custody.

9.1 Chain of Custody Procedures

- Document who collected the evidence, when, where, and the method used
- Each evidence transfer must be logged with date/time, from/to, purpose, and signatures
- Evidence must be stored in a secure, access-controlled location with tamper-evident seals
- Maintain a chain of custody log for each piece of evidence — physical or digital
- Only authorized CSIRT members may access evidence; access must be logged
- Evidence integrity must be verified using cryptographic hashes (SHA-256) at collection and each transfer

9.2 Forensic Imaging

- Create forensic images (bit-for-bit copies) of all affected system drives
- Use write-blockers when imaging to prevent evidence contamination
- Calculate and record hash values (SHA-256) of source and image to verify integrity
- Label all media with case number, date, system identifier, and analyst name
- Store original media separately from working copies — never analyze originals

- Capture volatile data (RAM, running processes, network connections) BEFORE imaging
- Document all tools used and their versions for forensic defensibility

9.3 Evidence Storage

- Physical evidence — Locked evidence cabinet with access log; climate-controlled environment
- Digital evidence — Encrypted storage on dedicated forensic server with access controls
- Retention period — Minimum 90 days per DFARS; extend to 1 year for SEV-1/SEV-2 incidents
- Off-site backup — Encrypted copy at secure secondary location
- Disposal — Evidence disposed of only after retention period and written authorization from Legal Counsel

9.4 Legal Hold

- Legal Counsel may issue a legal hold requiring preservation of all evidence related to an incident
- Legal hold supersedes standard retention schedules — do NOT destroy held evidence
- Legal hold applies to all forms: system images, logs, emails, documents, backups
- All CSIRT members and IT staff will be notified of legal hold requirements
- Legal hold remains in effect until formally released by Legal Counsel in writing

Appendix A: Incident Report Form

Complete this form for every security incident. Submit to IR Manager within 4 hours of detection for SEV-1/SEV-2, within 1 business day for SEV-3/SEV-4.

Incident ID	INC-YYYY-NNN (auto-assigned)
Date/Time Detected	
Date/Time Reported	
Reported By	
Reporter Contact	Phone: Email:
Severity Level	SEV-1 Critical SEV-2 High SEV-3 Medium SEV-4 Low
Systems Affected	

CUI Involved?	☐ Yes ☐ No ☐ Unknown If Yes, CUI Category: _____
Contract(s) Affected	
Incident Description	
Initial Actions Taken	
DFARS Reportable?	☐ Yes ☐ No ☐ Under evaluation Determined by: _____
Assigned To	

Appendix B: Key Contact List

Maintain this contact list current. Review and update at least quarterly. All contact information is classified as sensitive — do not distribute outside the CSIRT.

Internal Contacts

ROLE	NAME	PHONE	EMAIL
IR Manager	[Name]	[Phone]	[Email]
Lead Analyst	[Name]	[Phone]	[Email]
Communications Lead	[Name]	[Phone]	[Email]
Legal Counsel	[Name]	[Phone]	[Email]
IT Operations Lead	[Name]	[Phone]	[Email]
Executive Sponsor	[Name]	[Phone]	[Email]
CISO / Security Dir.	[Name]	[Phone]	[Email]
Facility Security Off.	[Name]	[Phone]	[Email]

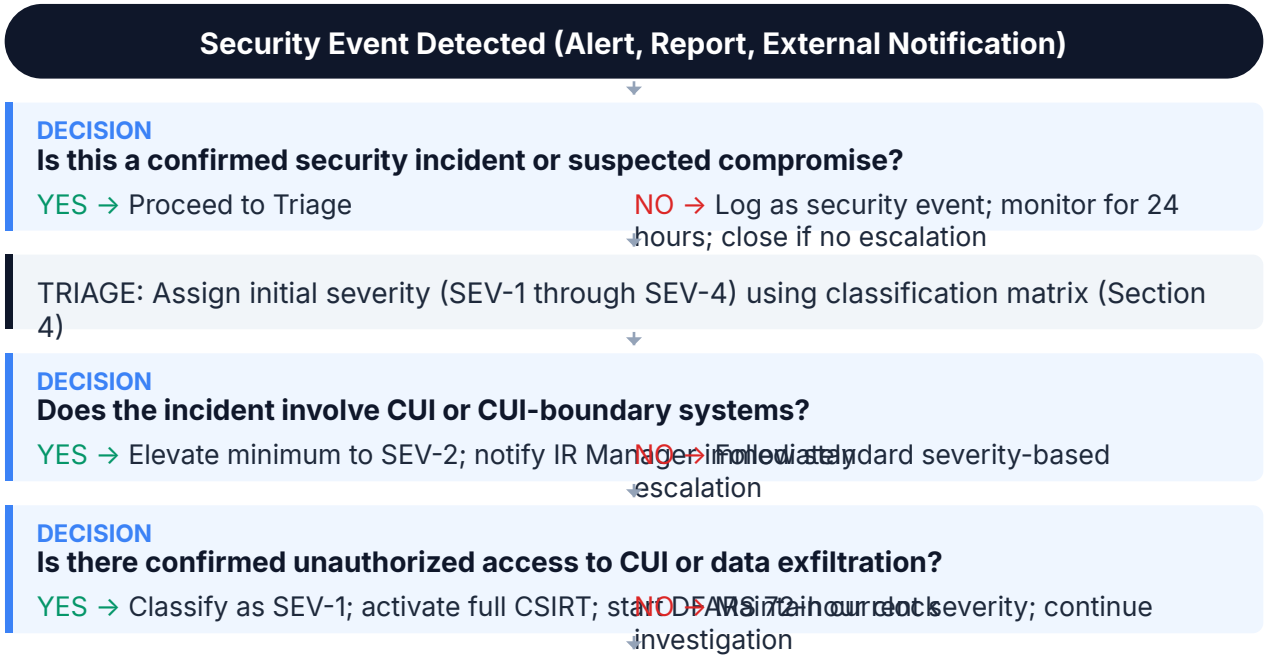
External Contacts

ORGANIZATION	PURPOSE	CONTACT INFORMATION

ORGANIZATION	PURPOSE	CONTACT INFORMATION
DC3 — DCISE Portal	DFARS cyber incident reporting	https://icf.dcise.cert.org
FBI Cyber Division	Criminal cyber activity	Local field office: [Number]
CISA	Critical infrastructure incidents	1-888-282-0870 / central@cisa.dhs.gov
Contracting Officer	Contract notification	[Name] / [Phone] / [Email]
Forensic Provider	Third-party forensics	[Firm] / [Phone] / [Contract #]
Cyber Insurance	Claims / breach counsel	[Carrier] / Policy #: [Number]
Outside Legal Counsel	Breach legal guidance	[Firm] / [Phone]
Dominus Gray, LLC	V-CISO advisory support	odie.gray@dominusgray.com

Appendix C: Escalation Flowchart

The following decision tree guides the escalation process from initial event detection through resolution. Follow the path based on answers to each decision point.



CONTAIN: Execute containment actions per Section 5.3; preserve evidence per Section 9

↓

DECISION
Is the incident a reportable "cyber incident" under DFARS 252.204-7012?

YES → Initiate DCISE portal reporting process (Section D); notify Contracting Officer

NO → Document determination rationale; continue response

↓

ERADICATE & RECOVER: Remove threat, restore systems, validate controls (Sections 5.4–5.5)

↓

POST-INCIDENT: Conduct lessons learned; update IRP; file final reports (Section 5.6)

↓

Incident Closed — Archive all documentation and evidence per retention policy