SOVEREIGN INTERNATIONAL METALS & ALLOYS, INC.

4990 SE Tower Dr.
Stuart, FL 34997 U.S.A
PHONE: (563)-355-2722
FAX: (563)-359-7984
E-MAIL: Alloys@simametals.net

Security Incident Response Plan

1.0 PURPOSE

This document is meant to provide Sovereign International Metals & Alloys, Inc.. ("SIMA") with an actionable plan for the identification, containment, and eradication of Security Incidents. This plan is to be used during the analysis of an incident and throughout the process of Security Incident detection and response.

1.1 SCOPE

This plan applies to all of SIMA' information systems, networks, and assets that create, store, receive, and/or transmit Confidential Information. This plan also applies to all of SIMA' paper records that contain Confidential Information.

1.2 TERMS

Capitalized terms herein shall have the meaning defined below:

Security Incident means any malicious act or suspicious event that compromises, is an attempt to compromise, or results in an actual or potentially adverse effect on (a) Confidential Information, or (b) an information system storing or providing access to Confidential Information.

Security Breach means an unauthorized disclosure of Personally Identifiable Information to a third-party or an unauthorized internal use or access of Personally Identifiable Information.

Confidential Information means Personally Identifiable Information; confidential business information, including trade secrets, commercial or financial information, proprietary information, or other commercially sensitive information that is not ordinarily shared outside of SIMA; and Covered Defense Information. Confidential Information may exist in electronic, paper, and oral formats and may be maintained by SIMA' external vendors and service providers.

Covered Defense Information means unclassified Controlled Technical Information or other information, as described in the Controlled Unclassified Information (CUI) Registry, which requires safeguarding. (The CUI Registry may be accessed at the following link: http://archives.gov/cui/registry/category-list.html). Covered Defense Information is either:

(a) Marked or otherwise identified in the contract, task order, or delivery order provided to SIMA by or on behalf of the U.S. Department of Defense in support of SIMA' performance of the contract; or

(b) Collected, developed, received, transmitted, used, or stored by or on behalf of SIMA in support of SIMA' performance of the contract.

Controlled Technical Information is a subset of Covered Defense Information and generally means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. This term does not include information that is lawfully publicly available without restrictions.

Personally Identifiable Information means any information that identifies, or can be used to identify, an individual, including, but not limited to, (a) first and last names; (b) date of birth; (c) address; (d) telephone number; (e) email address; (f) online account information; (g) Social Security number; (h) driver's license number; (i) state identification card number; (j) other government-issued identification numbers; (k) health or medical information; (l) financial account number; (m) credentials that permit access to a financial account; (n) payment card information; and (o) any information that is combined with (a) through (n) within this definition.

Logbook means a document created and used by SIMA to capture all activities related to identification and response to a Security Incident.

2.0 GENERAL PROCEDURES

This section discusses procedures that are common for all types of Security Incidents.

2.1 DETECTING ANAMOLOUS ACTIVITY

An individual who becomes aware of an anomalous activity that impacts or has the potential to impact Confidential Information and/or a SIMA IT system shall *immediately* report the activity to SIMA Resource at **563-355-2722**. The loss or theft of physical media or devices (such as laptops, smartphones, and USB drives) or paper records that may contain Confidential Information or are used to conduct SIMA' business is an anomalous activity that must be reported. In the event that the SIMA Resource has not responded after one hour the reporting individual shall escalate the issue to SIMA Management at **973-308-3813**. The individual should refrain from initiating his or her own investigation into the anomalous activity unless authorized to do so by the SIMA owner.

Anomalous activity may be identified by the following internal and external sources:

Internal Sources:

- SIMA employees
- On-site subcontractors

External Sources:

- Vendors/service providers/off-site subcontractors

- Law enforcement officials
- Clients/customers
- News and media reports
- Members of the general public

2.2 ANALYZING ANAMOLOUS ACTIVITY

The SIMA Resource shall perform an analysis of the reported anomalous activity to determine whether the event is symptomatic of a potential Security Incident. The analysis shall be conducted in a timely manner. To perform the analysis, the IT Resource will review event data that may include, as applicable, system and network log files and error messages, intrusion detection system reports, employee emails, and documents stored on SIMA' file shares. The Resource may access any potentially impacted SIMA information system or Resource to gather event data for analysis. The IT Resource may also interview SIMA employees, independent contractors, contacts at vendors, and witnesses as needed to gather event data for analysis. All accessed IT systems, Resources, and interviews shall be documented in the Logbook.

If analysis of the anomalous activity suggests, in the professional judgment of the Resource, that a malicious act, compromise, or attempt to compromise a SIMA information system or Confidential Information has occurred, the Resource shall *immediately* report the event to SIMA Owner at **563-340-8700 and email address steve@SIMAmetals.net**. The following non-exhaustive list of criteria shall be used by the Resource as a guide to analyze the event and determine whether to report an event to the as a potential Security Incident:

- Is/Was the event a successful or attempted unauthorized logical access to a SIMA information system, including unauthorized data manipulation?

- Is/Was the event a successful or attempted attack that prevents or impairs the normal authorized functionality of a SIMA information system, including Denial of Service (DoS) and ransomware attacks?

- Is/Was the event a successful or attempted, automated or directed propagation of malicious code, including, but not limited to, computer viruses, worms, bots, and scanners?

- Is/Was the event a possible violation of SIMA policy, including, but not limited to, its information security policy, that could lead to a Security Incident or Security Breach?

- Did the event involve employees responding to social engineering and phishing attacks, accessing Confidential Information without an authorized business purpose, verbally discussing Confidential Information without an authorized business purpose, or sharing Confidential Information with unauthorized internal parties?

- Is/Was the event an attempted or successful unauthorized configuration change that reduces the security posture of a SIMA information system?

- Did the event involve the "spillage" of Confidential Information, or the transfer of Confidential Information to an information system that is not accredited or authorized for the appropriate security level?

- Was anomalous activity reported by a SIMA information technology provider, other vendor or independent contractor, or law enforcement officials as a suspected or confirmed Security Incident?

- Did the event involve the loss or theft of unencrypted laptops, flash drives, or other portable electronic media containing, or providing access to, Confidential Information?

- Did the event involve the loss or theft of paper records containing Confidential Information?

- Did the event involve the intentional or unintentional disclosure of Confidential Information to unauthorized external parties?

- Did the event involve the unauthorized modification or destruction of Confidential Information, whether it was intentional or unintentional?

- Did the event result in an inability to access Confidential Information for authorized purposes?

- Did the event involve the copying of Covered Defense Information to unauthorized media, such as electronic storage media or hard-copy, paper print-outs?

- Did the event result in an inability to provide one or more federal customers with operationally critical support, as described in the customer contract(s)?

The IT Resource will document the event analysis in the Logbook.

Some events may be classified by the Resource as explainable, "accepted" activities. Accepted activities shall still be logged by the Resource in the Logbook and reported to the Resource via email at steve@SIMAmetals.net as a reported, but not actionable, event.

2.3 DECLARING A SECURITY INCIDENT

The Owner will review the analysis and criteria evaluated in accordance with Section 2.2 and, if warranted, declare a Security Incident. The Owner is solely responsible for determining if an event gives rise to a Security Incident based on the event data and the Resource's analysis. The Resource and any designees will assist the Owner as needed throughout the event classification process.

The Owner or designee will document the determination as to whether the event constitutes a Security Incident in the Logbook.

2.4 FORMING A SECURITY INCIDENT RESPONSE TEAM

Upon declaring a Security Incident, the Owner or Designee shall form a Security Incident Response Team ("SIRT") by deciding which roles are needed on the team and identifying specific individuals to fill those roles. Depending on the nature and severity of the Security Incident, as determined by the Owner or Designee, the SIRT may have some or all of the roles listed below:

1. *Discovering Party*. Individual or group of individuals who discover the anomalous activity.

2. *On-call IT Resource*. Individual who determines that the anomalous activity should be reported to the Owner as a potential Security Incident.

3. *Legal Counsel*. Tasked with evaluating potential legal concerns related to the Security Incident and engaging outside experts. Tasked with evaluating reporting obligations, including, for example, state data breach notification laws and the 72- hour notification requirement under the General Data Protection Regulation.

4. *Company Leadership*. The Owner or designee tasked with the following responsibilities:

    - Oversees investigation into Security Incident and response activities and assigns tasks to SIRT members.
    - Ensures that investigation and response activities progress in a timely and expedient manner.
    - Determines timing for involving Legal Counsel, law enforcement, outside experts, and public relations.
    - Serves as final arbiter when consensus cannot be reached on how to proceed with response activities.
    - If applicable, determines when SIMA' cyber-liability insurance carrier should be contacted.
    - Ensures that a Security Incident involving or affecting Covered Defense Information is rapidly reported to the U.S. Department of Defense, as described in Section 2.10 below.
    - Ensures that any malicious software that caused a Security Incident involving or affecting Covered Defense Information is timely submitted to the U.S. Department of Defense, as described in Section 2.11 below.
    - Ensures timely responses to the U.S. Department of Defense's request for other information and equipment, as described in Section 2.11 below.
    - Serves as the point of contact, or designates a point of contact, for the U.S. Department of Defense following a Security Incident involving or affecting Covered Defense Information.

5. *Recorder*. Tasked with maintaining the Logbook and recording lessons learned.

6. *IT Staff*. Tasked with providing system-specific technical expertise for investigation and response activities, such as intrusion counteraction, damage analysis, restoration/repair, and collecting and evaluating security advisories that are specific to affected system(s).

7. *Public Relations*. Tasked with coordinating communications to internal and external parties related to Security Incident, with final approval of any such communications by Company Leadership.

2.2 ESTABLISHING INTERNAL COMMUNICATION CHANNELS

The Recorder shall immediately open a telephone conference bridge that shall remain open for the duration of the Security Incident investigation and response efforts. The Recorder shall distribute the call-in information for the conference bridge via email to the SIRT. If, however, SIMA' email infrastructure is compromised or otherwise impacted by the Security Incident, then the Recorder shall distribute the call-in information for the conference bridge via telephone.

Email communications related to the Security Incident are permitted only to the extent that SIMA' email infrastructure was not compromised or otherwise impacted by the Security Incident. If email is not an appropriate communication channel, then communications related to the Security Incident will be made via telephone, in-person meetings and/or paper correspondence.

As needed, Company Leadership shall consult with Legal Counsel regarding guidelines for internal communications about the Security Incident.

2.3 HANDLING EXTERNAL COMMUNICATIONS

At any time, Company Leadership may contact third-party Resources to assist with performing activities outlined in this plan. A list of contacts available to support SIMA' response to a Security Incident is set forth in Appendix A.

It is important to maintain control of information during the course of a Security Incident investigation and response or analysis of a possible Security Incident. Providing incorrect information to the wrong people can have undesirable ramifications, particularly if the news media is involved. All release of information related to a potential or actual Security Incident—whether internally to other SIMA employees or externally to the media or third parties—must be authorized by Public Relations and/or Company Leadership.

Specific information related to a potential or actual Security Incident, such as the affected accounts, programs, or system or the nature of the Confidential Information involved, shall not be provided to any employees that are not part of the SIRT, unless authorized to

do so by Public Relations and/or Company Leadership. Employees who learn about the incident should be instructed not to gossip about the incident or share information about the incident with third parties, including through social media posts.

When necessary, Public Relations will develop scripts for answering questions about the incident and/or a press release to disseminate to the media. All scripts and press releases should be approved by both Legal Counsel and Company Leadership.

All internal inquiries about whether a specific piece of information about the incident can be released should be addressed to Public Relations and/or Company Leadership.

2.4 CREATING A LOGBOOK

The logging of information by the Recorder is a crucial component of responding to a Security Incident, especially in situations that may eventually involve legal action. Logging of information is also necessary for opportunities to learn from the Security Incident and execution of this plan.

The implications of each Security Incident are not always known at the beginning of, or even during, identifying the incident and taking remediation steps. Therefore, a written log must be kept for all Security Incidents, and the information should be logged in a location that cannot be altered by others. If possible, manually written logs are preferable because electronic logs can be altered or deleted. If electronic logs are used, SIMA should ensure that they are protected by authentication controls such that unauthorized users cannot access them. Every log should be dated, timestamped, and signed by the Recorder. The logs may be supplemented by copies of written investigation notes, emails, and letters that are compiled or exchanged during the course of responding to the Security Incident.

Information should be recorded in the Logbook during the detection, investigation, containment, eradication and recovery, reporting, and post-incident activity phases of this plan. The types of information that should be recorded in the Logbook include, but are not limited to:

- The date and time on which the incident was first discovered by SIMA;
- The date(s) and time(s) on which subsequent incident-related events were discovered or occurred;
- The person or source who discovered the incident and how the incident was discovered;
- The location of the incident;
- Narrative description of the incident;
- The date and time on which SIMA declared the incident to be a Security Incident;
- If applicable, a description of the attack vectors used and vulnerabilities exploited to result in the Security Incident;

- Timeline of actions performed in execution of this plan and the person(s) performing each action;
- The dates, times, and persons involved in all conference bridges and other communications related to the Security Incident;
- The amount of time spent working on incident-related tasks;
- Names of persons interviewed or contacted in connection with the Security Incident, including employees and external Resources;
- Narrative description of the actions taken to investigate the root cause of the incident and the persons involved in the investigation;
- Descriptions and locations of evidence gathered during the investigation of the Security Incident, including explanations of the relevance of the evidence and how the evidence has been preserved;
- Chains of custody for evidence gathered during investigation of Security Incident, if applicable;
- The type(s) of systems, applications, networks, computers, servers, user accounts, or media that have been analyzed during the investigation of the Security Incident and whether they have been affected or compromised;
- The type(s) of Confidential Information affected by the Security Incident, if applicable;
- Whether the Confidential Information affected by the Security Incident was encrypted, if applicable;
- The number of persons whose Personally Identifiable Information was affected by the Security Incident, if applicable;
- Witness interview notes compiled during the investigation of the Security Incident;
- Narrative description of the corrective actions taken to contain the Security Incident, mitigate the harmful effects of the incident, and minimize the likelihood of the incident's reoccurrence;
- Description of safeguards that were in place prior to the Security Incident to protect the affected Confidential Information and/or information system(s);
- Whether law enforcement was involved in identifying and/or responding to the Security Incident and if so, whether law enforcement requested SIMA to delay making any legally required notifications of the incident;
- Any noteworthy comments, observations, or insights from SIRT members;
- List of additional security measures planned to be taken in response to Security Incident, if applicable;
- Name and signature of the Recorder.

Under some circumstances, it may be appropriate for Legal Counsel to assist with the development of the Logbook to ensure the preservation of information needed to evaluate possible legal issues. Company Leadership should consult with Legal Counsel regarding whether to involve Legal Counsel in the preparation of Logbook entries.

Logbook recording activities should not impede or delay the investigation, containment, eradication and contractually or legally required reporting of the Security Incident.

Moreover, SIMA should appropriately safeguard Logbook entries from unauthorized access, as they will contain sensitive information about the incident, identified vulnerabilities, and the individuals involved.

2.5 INVESTIGATING THE SECURITY INCIDENT

As soon as the SIRT is formed, the SIRT will begin investigating the Security Incident to examine its nature and scope, determine its root cause or source, and analyze its effects. Company Leadership shall consult with Legal Counsel regarding the role that Legal Counsel will play in the investigation.

Company Leadership will ensure that the investigation progresses in an expeditious manner. Company Leadership and/or designees shall establish timeframes and set expectations for the SIRT's completion of various investigation activities. Under no circumstances shall Company Leadership or other SIRT members allow the investigation to unreasonably languish or be delayed.

In many cases, the SIRT's investigation of the Security Incident will overlap with the containment, remediation, and reporting phases of this plan. Throughout the investigation, the Recorder will enter all pertinent facts, evidence, and findings in the Logbook, in accordance with Section 2.4 above.

Upon launching its investigation, the SIRT will immediately determine whether Covered Defense Information, or an information system storing or providing access to Covered Defense Information, was involved in the Security Incident. It is important to complete this step quickly because there are special reporting requirements for Security Incidents affecting Covered Defense Information, as described in Section 2.10 below.

As part of its investigation, the SIRT will take appropriate steps to identify, at a minimum, the following:

- The information listed in Section 2.4 above as items to include in Logbook entries;
- The names and contact information, including addresses, telephone numbers, and email addresses, of the individuals whose Personally Identifiable Information was affected by the Security Incident, if applicable;
- Strategies for containing the Security Incident; and
- Strategies for eradicating and recovering from the Security Incident.

2.6 CONTAINING THE SECURITY INCIDENT

The SIRT shall contain the information systems impacted by the Security Incident, if applicable, to prevent the expansion of its scope and magnitude. Most Security Incidents involving Confidential Information will require containment prior to eradication and recovery.

Company Leadership will ensure that containment occurs in a swift manner. Company Leadership and/or designees shall establish timeframes and set expectations for the SIRT's completion of various containment activities.

Containment procedures will vary according to the specific circumstances surrounding the Security Incident and the level of residual risk SIMA is willing to accept. Further, SIMA' contracts with customers may specify the containment steps to take with respect to incidents involving certain categories of Confidential Information. In such cases, the SIRT should perform containment activities that satisfy the terms of the contract(s).

Generally, the SIRT should adhere to the following containment procedures:

- Identify the location and/or owner of the system(s) currently known to be in scope of the Security Incident.
- Determine if relevant computer(s)/endpoint(s) need(s) to be blocked from accessing the SIMA network.
- If applicable, block a specific IP address/address range, protocol, or UDP/TCP port at the network border or some other network interface in order to prevent the propagation of malware or to protect the network from further attacks.
- If applicable, isolate an affected computer or server by either unplugging the network cable from the computer/server or segmenting the server. These approaches are preferable to shutting down the computer/server or wiping all data from the affected device, as it is important to preserve information and evidence for further analysis. For wireless devices, the wireless interface can be disabled while leaving the computer running.
- Perform containment activities on the affected system(s) to prevent further damage to the computer or the data residing therein.
- Change passwords on all accounts impacted by the incident, including passwords of affected system(s) and user account passwords.
- If the Security Incident involved the loss or theft of equipment or hard-copy paper documents containing Confidential Information, then attempt to retrieve and secure them.
- When possible and appropriate, perform remote-wipe on lost or stolen mobile devices containing Confidential Information.

While implementing the selected containment strategy, the SIRT should take precautions to preserve relevant evidence in accordance with Section 2.8 below.

2.7 ERADICATING AND RECOVERING FROM THE SECURITY INCIDENT

After a Security Incident has been contained, eradication may be necessary to eliminate adverse impacts caused by the Security Incident and mitigate any vulnerabilities that were exploited. During eradication, it is important to identify all affected information systems within SIMA and at third party infrastructure maintained on behalf of

SIMA so that they can be remediated. For some Security Incidents, eradication is either not necessary or is performed during recovery. Examples of eradication include deleting all malware from computers and systems and disabling user accounts that have been compromised.

Recovery activities include restoring systems to normal operation, confirming that the systems are functioning normally, and remediating vulnerabilities to prevent similar incidents. Recovery may involve such actions as restoring systems from clean backups, rebuilding systems from scratch, replacing compromised files with clean versions, installing patches, changing passwords, and tightening network perimeter security (such as firewall rulesets and boundary router access control lists).

Eradication and recovery procedures will vary according to the specific circumstances surrounding the Security Incident and the level of residual risk SIMA is willing to accept. Both eradication and recovery activities should be done in a phased approach such that remediation steps are appropriately prioritized.

Generally, the SIRT should adhere to the following eradication and recovery procedures:

- Identify the full scope of the incident and determine if additional analysis is needed.
- Determine if any affected information systems need to have memory, hard drive(s), or other media imaged to preserve evidence in accordance with Section 2.8 below.
- Estimate the duration of time the affected system(s) or operations will be in eradication and recovery and out of operation. If this is beyond the length of time that can be tolerated by SIMA or its customers, invoke business continuity/disaster recovery procedures to restore the system(s) or operations until normal operations can be resumed.
- Mitigate the attack vector to minimize the likelihood of further instances of the Security Incident. Mitigation efforts may include:
    - Patching vulnerabilities in the operating system and all software applications
    - Changing passwords
    - Placing a system behind a firewall or adjusting firewall rules
    - Updating or installing new security software, such as anti-virus software or a host-based personal firewall
    - Reviewing appropriateness of access rights associated with user accounts
    - Applying standard system security hardening techniques
    - Conducting a security assessment
    - Administering user training
- Return any affected systems to an operationally ready state.
- Confirm that any affected systems are functioning normally.

- If the Security Incident occurred at a subcontractor, ensure that subcontractor took appropriate corrective actions or consider terminating relationship with subcontractor.
- If necessary, implement additional monitoring to look for future related activity.

2.8 PRESERVING EVIDENCE AND SECURITY INCIDENT RESPONSE RECORDS

The SIRT shall take reasonable measures to capture and preserve evidence and records related to the Security Incident during the investigation, investigation, containment, eradication and recovery, and reporting phases. For example, in most cases, the SIRT should not wipe data from its affected systems and/or devices before ensuring that all appropriate evidence is first preserved. Company Leadership will consult with Legal Counsel to establish proper evidence handling and preservation procedures, including the appropriate retention period(s).

The following items are examples of evidence and records concerning the Security Incident that may need to be preserved in a forensically sound manner:

- Forensic disk images
- System log files
- Lists of network connections, processes, login sessions, open files, and network interface configurations
- Contents of memory
- Network monitoring/packet data
- Screenshots
- Photographs and video recordings
- Logbook entries
- Information and equipment necessary for a forensic analysis of the incident to be performed
- Malware that has been isolated
- Copies of communications and reports made pursuant to Sections 2.10 and 2.11 below.

If the Security Incident involves Covered Defense Information or an information system storing or providing access to Covered Defense Information, then the SIRT is required to preserve, at a minimum, the following items:

- Images of all known affected information systems (for at least 90 days from the submission of the Incident Collection Form to the U.S. Department of Defense, as described in Section 2.10 below);
- Relevant monitoring/packet capture data (for at least 90 days from the submission of the Incident Collection Form to the U.S. Department of Defense, as described in Section 2.10 below);

- Information, equipment, or media that is necessary to conduct a forensic analysis; and
- Malware associated with the Security Incident, if applicable.

The SIRT may also find it helpful to consult the National Institute of Standards and Technology, Special Publication 800-86: "Guide to Integrating Forensic Techniques into Incident Response" when strategizing the collection and preservation of evidence.

2.9 EVALUATING LEGAL ISSUES

Legal Counsel shall evaluate the nature of the Security Incident to ascertain contractual, state, federal, and regulatory obligations, including reporting requirements described in Section 2.10 below. SIRT members shall work diligently to respond to requests from Legal Counsel to provide information necessary to evaluate legal issues. Company Leadership will consult with Legal Counsel as appropriate and necessary during each phase of the Security Incident response process.

2.10 REPORTING THE SECURITY INCIDENT

Legal Counsel shall advise Company Leadership on whether the Security Incident triggers reporting obligations under state or federal laws or regulations or customer contracts. If Legal Counsel determines that SIMA is required to report the Security Incident to any third party, Company Leadership is responsible for ensuring that the report is made without unreasonable delay, and within the timeframe prescribed by the applicable law(s), regulation(s), or contractual provision(s). In some cases, a report may need to be made while the SIRT is still participating in the investigation, containment, or eradication and recovery phases of this plan.

Legal Counsel shall prepare or direct the preparation of any required report to ensure that its contents satisfy legal and/or contractual requirements. As needed, the preparer of the report will consult the Logbook and SIRT team members for information about the incident. Company Leadership will submit the required report(s) or delegate submission to Legal Counsel or other SIRT member.

There are special reporting requirements for Security Incidents affecting Covered Defense Information, an information system in which Covered Defense Information resides, or SIMA' ability to provide operationally critical support to its federal customer(s). Namely, SIMA must rapidly report such Security Incident to the U.S. Department of Defense, Cyber Crime Center (DC3) ***no later than 72 hours*** after SIMA discovers the Security Incident. A Security Incident is "discovered" on the day on which any SIMA employee or agent first learns about the incident, rather than on the day on which the IT Manager of Operations declares that the incident constitutes a "Security Incident."

Reports shall be submitted to the U.S. Department of Defense by accessing the Incident Collection Form at the following DIBNet portal: https://dibnet.dod.mil/portal/intranet/. At least the following information must be included in the Incident Collection Form:

- Company name
- Company point ofcontact information (address, position, telephone, email)
- Data Universal Numbering System (DUNS) Number
- Contract number(s) or other type of agreement affected or potentially affected
- Contracting Officer or other type of agreement point of contact (address, position, telephone, email)
- USG Program Manager point of contact (address,position, telephone, email)
- Contract or other type of agreement clearance level (Unclassified, Confidential, Secret, Top Secret, Not applicable)
- Facility Commercial and Government Entity Code (CAGE) code
- Facility Clearance Level (Unclassified, Confidential, Secret, Top Secret, Not applicable)
- Impact to Covered Defense Information
- Ability to provide operationally critical support
- Date incident discovered
- Location(s) of compromise
- Incident location CAGE code
- U.S. Department of Defense programs, platforms or systems involved
- Type of compromise (unauthorized access; unauthorized release, including inadvertent release; unknown; not applicable)
- Description of technique or method used in cyber incident
- Incident outcome (successful compromise, failed attempt, unknown)
- Incident/Compromise narrative
- Any additional, relevant information

After receiving the Incident Collection Form, the DC3 will assign the form a tracking number and send the form to the federal contracting officer.

2.11 SHARING INFORMATION WITH THE U.S. DEPARTMENT OF DEFENSE

Company Leadership or a designee shall serve as the point of contact for all communications with the U.S. Department of Defense described in this section and is responsible for ensuring that information is shared with the department in a timely manner. As necessary, Company Leadership or a designee will consult with Legal Counsel regarding sharing information with the DC3.

If a Security Incident that SIMA reports to the U.S. Department of Defense under Section 2.10 above was caused by or otherwise involved malware, then the SIRT shall isolate the malware and submit the malware to the DC3 in accordance with instructions that DC3 or the federal contracting officer will provide to SIMA. SIMA should *not* send the malware directly to the contracting officer. The DC3 will then analyze the submitted malware.

The DC3's instructions for submitting malware will resemble the following, but may vary on a case-by-case basis:

- To send malicious code samples to DC3, use a web browser to access the Malware Submission Form at https://dcise.cert.org/icf/.
- Include the following information:
    - First name and last name
    - Email address
    - Company name
    - Location
    - Incident Collection Form Number (if applicable), e.g. ICF 14123-001
    - Description of how the malware sample relate to the submitted ICF and/or provide other information describing the reason for submission
- Select the malicious code sample to upload. If uploading multiple files, add all files to a compressed archive prior to submitting.
- Click the "Submit" button at the bottom of the form.
- In the event that the Malware Submission Form is not available, or if other circumstances prohibit the submission of malicious code samples via the web form, contact DCISE@dc3.mil for assistance.

Additionally, the DC3 may request access to images of all known affected information systems and relevant monitoring/packet capture data during the 90-day period following its receipt of the Incident Collection Form. In some cases, the DC3 will decline interest in receiving such information. The SIRT should be prepared to submit such information to the DC3 upon request.

The DC3 may also request access to additional information or equipment necessary to conduct a forensic analysis. Further, the department may request materials to perform a cyber-incident damage assessment. Therefore, the SIRT should preserve pertinent evidence and records in accordance with Section 2.8 above. While preserving the evidence and records, the SIRT should identify and mark any business confidential/proprietary information and Personally Identifiable Information to assist the U.S. Department of Defense in protecting such information against unauthorized access.

The DC3's instructions for submitting images, monitoring/packet capture data, and additional information or equipment (collectively, "media") will resemble the following, but may vary on a case-by-case basis:

- For those instances in which all the files containing unclassified Controlled Technical Information (CTI) that are part of the compromise can be identified, submit a copy of each file containing unclassified CTI associated with the compromise.
- If all the files containing unclassified CTI associated with the compromise cannot be identified, then a bit for bit image can be submitted. In these cases, the

preparation of the drive image(s) should be as follows for submission. Create the image on a separate wiped hard drive, where the hard drive is overwritten using a suitable application or hardware that overwrites previous data with a pattern of binary data. The hard drive can be wiped with utilities such as Unix 'dd' application or other commercially available hard drive duplicators with a drive wiping feature. Suitable applications for creating drive images include, but are not limited to, the following: (a) Guidance Software's EnCase (software); (b) Access Software's FTK Imager (software); (c) Open source dd application (software); and (d) hard drive duplicator (hardware).

- When submitting the media, create a cover letter that includes the following information:
  - Incident Collection Form report number
  - Description of the type and number of media being submitted, along with make, model, and serial numbers and/or other identifying information as appropriate
  - Explanation of how the media relate to the Security Incident. This description should provide context to the media submission and not simply repeat the incident summary reported in the Incident Collection Form.
  - MD5 hash results for each item submitted
- Send the cover letter and media via registered USPS mail, FedEx, UPS, or agency drop to: DIBCERT (DCISE MAC); 911 Elkridge Landing Rd.; Linthicum, MD 21090-2993
- Send a digitally signed email to dcise@dc3.mil indicating media have been shipped. The subject line should read, "Media submission for [incident number]." If the image files are password-protected, include the password in this email.
- Upon receipt of the media, DC3 will send an email confirming its receipt.

3.0 POST-INCIDENT ACTIVITY

3.1 IDENTIFYING LESSONS LEARNED

Within a reasonable time following the handling and resolution of a Security Incident, Legal Counsel should reconvene the SIRT to lead a postmortem analysis of the response efforts. All involved parties or their designees should meet to discuss actions that were taken in response to the incident and the lessons that were learned. The team should consider at least the following:

- How effective was SIMA in detecting and responding to the incident?
- How effective were the communications channels used by the SIRT during incident response activities?
- Were any mistakes made during the response process, and if so, how can such mistakes be avoided in the future?
- What was the root cause of the Security Incident? How effective were the corrective actions that were taken? What is SIMA plan to reduce the likelihood of the incident's reoccurrence?

- How well did SIRT members perform their roles? Was the SIRT sufficiently staffed? Should any roles be minimized or expanded?
- How well were the detection and response efforts documented in the Logbook?
- Did the SIRT contact law enforcement? If so, was the timing for contacting law enforcement appropriate? If not, should the SIRT have contacted law enforcement?
- What additional tools and Resources are needed to better identify, analyze, contain, and eradicate future incidents?
- Were internal and external communications regarding the incident adequately handled?
- How effective is this plan and other existing informal and formal procedures? What modifications are needed, if any?

When appropriate, a set of recommendations based on the discussion should be documented and presented to Company Leadership.

3.2 INFORMATION SHARING

The SIRT may consider voluntarily sharing information about the Security Incident with the following external Resources, if these Resources were not already consulted during the response process:

- Cyber-liability insurance carrier
- A sector-specific Information Sharing and Analysis Center (ISAC), such as the Defense Industrial Base ISAC or Defense Security Information Exchange. A list of ISACs can be accessed at the following link: https://www.nationalisacs.org/member-isacs
- Multi-State Information Sharing and Analysis Center (MS-ISAC)
- Federal Bureau of Investigation (FBI) field office
- FBI Infraguard. Information about local chapters can be accessed at the following link: https://www.infragard.org/
- U.S. Secret Service field office
- United States Computer Emergency Readiness Team (US-CERT)
- Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
- U.S. Department of Defense, Defense Industrial Base Cybersecurity Information Sharing

Appendix A

SIMA' Security Incident Response Plan Contact List

Karen Deem, KAD@simametals.net	**(563) 355-2722 (work)**	**(563) 343-0368 (mobile)**