DIB CS/IA Incident Collection Form

Detailed Instructions

Part I: Type of Report

Cyber incident: Actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing.

- Select the appropriate option:
  - Initial Incident: Select this option for initial incident reporting.
  - Follow-on Report: Select this option for follow-on reporting.
  - Indicator only: In some situations the submitter would like to provide information to be shared with DoD and other DIB participants. This option is used to report suspicious cyber activities that might be important, but do not meet the level of a cyber incident. Select this option for indicator only reporting, and complete only the indicator part of the form.

Incident Summary Information

Section II: DIB Partner Point of Contact

This section collects information for DC3/DCISE to contact the reporting partner regarding the reported incident. The DIB partner point of contact is a cleared individual identified and authorized to work directly with DC3/DCISE on cyber incident sharing and reporting. Enter the contact information of the individual that DC3/DCISE should contact regarding questions or feedback about the report.

- **Last name -** Enter the last name of the appropriate DIB partner point of contact.
- **First name -** Enter the first name of the appropriate DIB partner point of contact.
- **Email -** Enter the primary work email address of the appropriate DIB partner point of contact.
- **Company name -** Enter the name of the company that employs the DIB partner point of contact.
- **Location -** Enter the full postal mailing address for the work location of the DIB partner point of contact.
- **Phone -** Enter the daytime phone number of the appropriate DIB partner point of contact, including the country and area code (+x xxx-xxx-xxxx).
- **Fax -** Enter the daytime fax number of the appropriate DIB partner point of contact, including the country and area code (+x xxx-xxx-xxxx).
- **Division / group -** Enter the division or group in which the DIB partner point of contact works.
- **Time Zone -** Select the time zone in which the DIB partner point of contact resides.
- **Provide additional POC information as appropriate** (Click on POC link). If additional POCs are needed, select the appropriate category (incident response, technical or business unit points of contact). A new window will be presented to collect the additional POC information with the same fields as above.

Section III: Incident Identification

- **Incident Collection Form (ICF) number** - The DC3/DCISE will assign a unique identifier for tracking the incident report. The format of the identifier will be YYDDD-NNN, where YY equals the last two digits of the year, DDD is the day of the year, and NNN is the sequential report number (e.g., 10020-001). This number should be auto generated for a new report. For a follow-up report, enter the assigned DC3/DCISE number.
- **Reporting timestamp (UTC)** - Enter the date and time that this report was submitted to the DC3/DCISE, using the UTC time zone and formatted as DD/MM/YYYY hh:mm (24 hour format).
- **Partner tracking or incident number** - Enter any internal tracking numbers that your organization is using to track the reported incident.
- **Disseminate partner tracking or incident number?** Select the appropriate option to indicate whether the number entered as a response to the previous question should be included in the partner report generated by the online Incident Collection Form (ICF) system.
- **Other government organization tracking numbers -** If this incident has been reported to any other government organization (such as US-CERT, DSS, FBI, DoD agencies), enter the name and tracking numbers of the organization(s).
- **Do you required pre-publication review of the Customer Response Form (CRF)**? Following the submission of an ICF, DC3/DCISE will develop a customer response report as a means to provide analytical information back to the submitter. If the submitter would like to review the anonymized report before it is shared with other DIB Partners, select “Yes”. The submitter will be provided the opportunity to review the report before it is released in final form to the entirety of the partnership. If no inputs are received within two federal business days from the time DC3/DCISE requests review, the lack of input will be logged, and the report published. If "No" is selected, the submitter will not be contacted for comments prior to release.

Incident Detail Information

Section IV: Report Submission Tier and Categorization

This section gathers information to characterize the reported incident. Select the appropriate tier level and category (or categories) that apply to the incident.

- Describe the reason for submitting this report by selecting *one* of the following options below: - Choose the tier that best describes the incident. If unknown, select “not determined at this time”.

  APT activity is defined as (1) activity related to or found as a result of specific items marked as APT in the DC3/DCISE cyber threat information products, or reported as APT by any other government sources, *or,* (2) activity the DIB Partner believes to be APT based on profiles provided in cyber threat information products, or reported as APT by other government sources, or from its own research, including:

  - Tier 1a: APT and DoD systems or data involved.
  - Tier 1b: APT and systems or data involved unknown.
  - Tier 1c: APT and no DoD systems or data involved.
  - Tier 2: Successful DoD program targeted intrusion, non-APT, encompassing activities that do not fall into Tier 1.

- Tier 3: Incidents that do not fall into Tiers 1 or 2 and may be of interest to the cyber community (e.g., PDA exploits).
- Not determined at this time.

- **Categorize this incident.** Select *as many* of the following options that apply:

- CAT 0 - Situational Awareness Only: The partner is providing this information for situational awareness only and is not expecting a response from DC3/DCISE.
- CAT 1 - Root-Level Intrusion: This category indicates unauthorized privileged access to a system. Privileged access, often referred to as administrative or root access, provides unrestricted access to the system. This category includes unauthorized access to information or unauthorized access to account credentials that could be used to perform administrative functions (e.g., domain administrator). If the system is compromised with malicious code that provides remote interactive control, report it in this category.
- CAT 2 - User-Level Intrusion: This category indicates unauthorized, non-privileged access to a system. Non-privileged access, often referred to as user-level access, provides restricted access to the system based on the privileges granted to the user. This includes unauthorized access to information or unauthorized access to account credentials that could be used to perform user functions such as accessing web applications, web portals, or other similar information resources. If the system is compromised with malicious code that provides remote interactive control, report it in this category.
- CAT 3 - Unsuccessful Activity Attempt: This category addresses deliberate attempts to gain unauthorized access to a system that is defeated by normal defensive mechanisms. For example, if an attacker fails to gain access to the system (i.e., attacker attempt valid or potentially valid username and password combinations), and the activity cannot be characterized as exploratory scanning. Reporting these incidents is critical for gathering useful effects-based metrics and situational awareness.
- CAT 4 - Denial of Service: The activity denies, degrades, or disrupts the normal functionality of a system or network.
- CAT 5 - Non-Compliance Activity: The activity potentially exposes systems to increased risk as a result of the action or inaction of authorized users. This includes administrative and user actions, such as failure to apply security patches, connections across security domains, installation of vulnerable applications, and other breaches of policy. Reporting these incidents is critical for gathering useful effects-based metrics.
- CAT 6 - Reconnaissance: The activity seeks to gather information used to characterize systems, applications, networks, and users that may be useful in formulating an attack. This includes activity such as mapping networks, systems devices and applications, interconnectivity, and their users or reporting structure. This activity does not directly result in a compromise.
- CAT 7 - Malicious Logic: This category addresses installation of software designed and/or deployed by adversaries with malicious intentions for the purpose of gaining access to resources or information without the consent or knowledge of the user. This only includes malicious code that does not provide remote interactive control of the compromised system. Interactive access may include automated tools that establish an open channel of communications to and/or from a system.
- CAT 8 - Investigating: These incidents are potentially malicious or anomalous activity deemed suspicious and warrant, or are undergoing, further review.
- CAT 9 – Explained Anomaly: These suspicious incidents are determined to be non-malicious activity and do not fit the criteria for any other categories. This includes incidents such as system malfunctions and false alarms. When reporting these incidents, specify the reason for which it cannot be otherwise categorized.

- **Provide additional information.** If possible, explain why this incident matches the tier level and categories selected above. Include references to any reporting that may have initiated this action, such as vendor alerts, news stories, or previous DC3/DCISE or other governmental reporting. Also include the specific indicators that were used to identify the activity.
- **Incident Impact.** Select the best answer for the impact of this incident on your organization as known at the time of reporting.
  - None: No adverse affect
  - Low: Limited adverse affect
  - Moderate: Serious adverse affect
  - High: Severe or catastrophic adverse affect.

Section V: Incident Description

- Provide a detailed description of this incident. Include summary of the activity, node and data involved, and impact. This section will be used for DC3/DCISE only, so attribution information may be included.
- Provide as much information as possible without attribution information so that it can be shared with others for situational awareness.

Section VI: Data Compromise Details

- **Was data compromised?** – Indicate whether you believe there was unauthorized access to information or an information system. Select "Yes", "No", or "Unknown."
- **If known, select all data compromise types that apply** - Choose the appropriate answer by marking the checkbox.
  - Data confidentiality (e.g., data was viewed)
  - Data integrity (e.g., data was altered)
  - Data availability (e.g., access to data was prevented, DDOS)
  - Data loss (e.g., data deleted)
- **If the data was compromised, was the data associated with a DoD compartment or program? -** Select "Yes", "No", or "Not yet determined."
- **If the answer to previous question is yes, identify the DoD component and or Program** (e.g., Military Department / Program) **-** Enter the name of the affected DoD component or program (Army, Navy, etc.).
- **Type of information affected** (e.g., financial, human resources) – Enter the type of data that was affected.

Section VII: Additional Information

- **Does the identified attack vector appear in open source research? -** This question determines if the initial attack vector appears in publicly available information or is widely known.
- **Does this activity represent a shift in tactics, techniques, and procedures (TTPs) from previously known APT profiles? -** This question is intended to determine if the reporting partner believes that this activity represents a shift in the TTPs being used by a known APT profile.

- **Approximate staff time to recover from the activity** - Enter the amount of staff time (in hours) that was required to recover from the activity. For example, two employees working 4 hours each would total 8 hours.
- **Would you like to provide additional information regarding observations?** - If yes, please complete the observation form provided in a new window.

OBSERVATION INFORMATION (SUPPLEMENTAL)

An observation is an individual instance of the activity that either solely, or in combination with other observations, comprises the entire incident being reported. Observations provide the information necessary to characterize, identify, and contain the activity.

Section I: Incident Observation

- **Observation number.** This will be auto-generated.
- **Reporting timestamp.** This will be auto-generated.
- **Partner observation identification.** Enter any internal tracking numbers that your organization is using to track the reported observation. If you do not have one, leave blank.
- **Provide a detailed description of this observation.** Include a summary of the activity, node and data involved, and impact. This section will be used for DC3/DCISE only, so attribution information may be included.
- **Provide a detailed description of this observation that can be shared outside the DC3/DCISE.** Include a summary of the activity that does not include attribution information so that is may be shared with other DIB Partners and government stakeholders.

Section II: Incident Information - Detection and Response

- **Detection Method:** Select all methods used to detect the incident.
  - Email Gateway Monitoring: detected through the use of email content filtering or the review of email logs
  - Log Review: detected through manual or automated review of system log files (e.g., firewall logs)
  - Network –based IDS: detected through signatures on network intrusion detection system
  - Network –based IPS: detected through signatures on network intrusion prevention system
  - ISP Operated Sensor: detected by Internet service provider monitoring
  - Honeypot/Decoy device: detected through use of honeypot or decoy device
  - Proactive detection/audit: detected during system or security audit
  - Internet Proxy Monitoring: detected via proxy alert
  - User Interface/Browser: detected via alert from local operating system or local internet browser
  - Human: detected via employee or other individual witnessing malicious or suspicious activity
  - Anti-virus/Malware: detected via alert from anti-virus product or heuristic-based detection application
  - Host-based IDS: detected through signatures on host intrusion detection system
  - Security Event and Information Manager: detected through rules built into the Security Event and Information Manager system

  - Host-based IPS: detected through signatures on host intrusion prevention system
  - Other
- **Outcome: Select the appropriate option to identify the outcome of the incident.**
  - Successful Compromise – The attacker was able to gain unauthorized access to information or information systems.
  - Failed Attempt – The attacker was unable to gain access to information or information systems.
  - Unknown – The affects of the attempted attack are not currently understood.
- **Response Actions: Select all action taken.**
  - No action taken: no actions deemed necessary for this incident
  - Contacted target site: contacted the site(s) identified as the target of the activity
  - Investigating: reviewed data to determine extent of incident
  - Blocked source network: blocked the originating IP address(es)
  - Rate limit from source host: limited the amount of bandwidth that can be used to/from the source host
  - Rate limit network protocol/port: limited the amount of bandwidth that can be used to/from the protocol or port
  - Triaging reports: collected data regarding this incident
  - Contacted attack source site: contacted the site(s) identified as the source of the activity
  - Contacted originator: contacted the individual who owns the account that may have originated the activity
  - Blocked host: blocked all communications to/from specific host or network
  - Blocked network protocol/port: blocked all communications to/from a specific protocol or port
  - Rate-limit traffic from source network: limited the amount of bandwidth that can be used to/from the source network
  - Receiving additional information: anticipating the receipt of additional information based on ongoing analysis
  - Other
- **Incident start date and time:** Provide the date the incident began formatted as DD/MM/YYYY (hh:mm in 24 hour format).
- **Incident start timezone:** Select from pull down menu.
- **Initial observation date and time**: Provide the date the incident was observed formatted as DD/MM/YYYY (hh:mm in 24 hour format)
- **Initial observation timezone:** Select from pull down menu.
- **Incident resolution date and time:** Provide the date the incident was resolved, formatted as DD/MM/YYYY (hh:mm in 24 hour format).
- **Incident resolution timezone:** Select from pull down menu.
- **Do you have media or malware that you will be submitting for DC3/DCISE analysis?** Indicate whether you have any drives, drive images, logs, malware samples, or any other pertinent technical data to be analyzed by DC3/DCISE. These items should be submitted separately from this form, in accordance with DC3/DCISE media and malware submission processes.

- **Were specific systems targeted?** Attempt to identify specific systems that appear to have been targeted in the attack, then select yes. A separate window will be provided to collect information related to that target.
- **Was this activity detected by a DC3/DCISE-provided indicator?** This answer determines whether this activity was detected by a DC3/DCISE-provided indicator.

HOST INFORMATION (SUPPLEMENTAL)

- **Tracking Number:** This will be auto-generated.
- **Report Time:** This will be auto-generated.
- **Partner Host Identification:** Enter any internal tracking numbers that your organization is using to track the reported observation. If you do not have one, leave blank.
- **Was this a targeted host or malicious/attacking host?**
  - Unknown
  - Source - This host is the source in this incident.
  - Intermediate - This host plays an intermediate role in this incident.
  - Target - This host is the target in this incident.
- **IP Address or IP Address Range:** IP address of host or range of IP addresses. IP address format is xxx.xxx.xxx.xxx. IP address range format is xxx.xxx.xxx.xxx-zzz.zzz.zzz.zzz.
- **System Name or System Names:** Internal and/or external name(s) of system
- **DNS name or DNS names:** Complete name of system (e.g. system1.domain.com)
- **Resolution Time:** If this system's involvement in the incident has been resolved, please specify time/date of resolution.
- **Is the affected system/node (or services) significant to the operation of the organization or infrastructure?** Select "Unknown", "Yes", or "No"
- **Host Functions:** What is the role of this system on your network; what services does this system provide? (Select all that apply)
  - End user system - The host functions as an end user system
  - Publicly accessible server - The host functions as a publicly accessible server
  - Email server - The host functions as an email server
  - Streaming-media server - The host functions as a streaming-media server
  - File server (e.g., SMB, AFS, SVN) -The host functions as a file server
  - Peer-to-peer node - The host functions as a peer-to-peer node
  - Directory server (e.g., LDAP, whois) -The host functions as a directory server
  - Print server - The host functions as a print server
  - Database server - The host functions as a database server
  - Log server - The server functions as a log server
  - Corporate application server - The server functions as a corporate application server

  - Hardware/software release or repository - The server functions as a hardware/software release or repository
  - Manufacturing controller - The server functions as a manufacturing controller
  - License server - The server functions as a license server
  - Internal-use-only server - The server functions as an internal-use-only server
  - Web content server - The server functions as a Web content server
  - Instant messaging server - The server functions as an instant messaging server
  - Voice (e.g., SIP, H.323) -The server functions as a voice server
  - File Transfer Protocol (FTP) - The server functions as a file transfer protocol server
  - Name server (e.g., DNS, WINS) -The server functions as a name server
  - Authentication Server (e.g., Kerberos, Active Directory) -The server functions as an authentication server
  - Application server - The server functions as an application server
  - Infrastructure (e.g., router, firewall) -The server functions as an infrastructure server
  - Unknown - The server functions as an unknown server
  - Lab or development system - The server functions as a lab or development system
  - Engineering/development - The server functions as an engineering/development system
  - Business development or sales system - The server functions as a business development or sales system
  - Marketing system - The server functions as a marketing system
  - Sensor - The server functions as a sensor system

- **Host Operating System (major):** What is the main operating system running on this system?
  - Microsoft Windows
  - UNIX / Linux
  - Unknown
  - Apple Mac OS
  - Other - Please type in the operating system in the given space.
- **Host Operating System Version:** What version of the main operating system is running on this host (e.g. Service Pack version for Windows)
- **Is this a Virtual Machine?** Is this a virtual machine or is this a host of multiple virtual machines?
- **If yes to previous question, were any virtual machines affected by this event?** If there are technical indicators that you feel can be used by others within the community to detect similar activity, select the group of indicators to report. You will be presented with an additional page to submit individual indicators from this report.
- **Host State:** Explain the state of this host as it pertains to this incident. Select all that apply.
  - Spoofed: This domain or system did not participate in this incident, but its address space or DNS name was forged.
  - Innocent, compromised: The system typically serves a legitimate purpose, but was compromised and used in a fraudulent manner in the reported incident.
  - Unknown: It is unclear how the system or domain was involved in this incident.

  - Fraudulent: This system was deployed solely for the purpose of hosting a fraudulent site intended to misguide a user.
  - Innocent, hijacked: The IP Address or domain name typically serves a legitimate purpose, but was hijacked and used in a fraudulent manner in the reported incident.
  - Other.

- **Physical Location of Node:** Where is this node located (network, business unit, city, state, country).
- **CAGE Code:** Enter the Commercial and Government Entity (CAGE) code for the facility in which the incident occurred. Note: in some cases the facility may not have a CAGE code.
- **Additional Information:** Give further details about the host that were not covered in previous sections.
- **Are there additional targeted or attacker systems?** If there are other systems involved in this incident, select yes to begin a new host page.

INDICATOR INFORMATION (Supplemental):

Identify the type of indicator you are reporting on by selecting the appropriate indicator (Network, Signature, Registry, Email, File, String, Block of indicators, or None). Based on that selection the appropriate page will be presented for completion.

Network Indicator Information (Supplemental)

- **Indicator Type:** Select Network.
- **Indicator Sub-Type:** Select one of the following Indicator types.
  - IPv4Address - This is the IPv4 Address of the system. The format is to be dot-decimal notation (e.g., 192.168.1.1).
  - IPv4RangeStart - This is the IPv4 Address that marks the beginning of the range given to the system or network. The format is to be dot-decimal notation (e.g., 192.168.1.1).
  - IPv4RangeEnd - This is the IPv4 Address that marks the ending of the range given to the system or network. The format is to be dot-decimal notation (e.g., 192.168.1.1).
  - IPv6Address - This is the IPv6 Address of the machine. The format is to be a 128 bit hexadecimal, colon separated string (e.g., 2001:db8:85a3::8a2e:370:7334).
  - IPv6RangeStart - This is the starting IPv6 Address of the machine. The format is to be a 128 bit hexadecimal, colon separated string (e.g., 2001:db8:85a3::8a2e:370:7334).
  - IPv6RangeEnd - This is the ending IPv6 Address of the machine. The format is to be a 128 bit hexadecimal, colon separated string (e.g., 2001:db8:85a3::8a2e:370:7334).
  - application protocol - The layer seven protocol used to establish process-to-process communications (e.g., HTTP, DNS, SMTP).
  - port - A number describing the communications endpoints for the network traffic.
  - Transport protocol - The layer four protocol used to encapsulate data sent between application processes (e.g. TCP, UDP).
  - Encryption Type - A description of the encryption schema utilized to obfuscate the network traffic.
  - WhoIs - Registrant information retrieved from WHOIS database(s).
  - FQDN - This is the fully qualified domain name of the system.

- **Value:** Provide the value of the indicator
- **Description :**
  - Provide additional description as needed for indicators. This section will be used for DC3/DCISE only, so attribution information may be included.
  - Provide additional description as needed for indicators without attribution information so that it can be shared with others for situational awareness.
- **Are there additional indicators to report?** Select appropriate indicator (Network, Signature, Registry, Email, File, String, or None) and the appropriate page will be presented.

Signature Indicator Information (Supplemental)

- **Indicator Type:** Select Signature indicators.
- **Indicator Sub-Type:** Select one of the following Indicator types.
  - Signature Type: this is defined by the type of system or application that will utilize the signature (IDS, Anti-Virus, etc).
  - Signature String: a finite sequence of characters (i.e., letters, numerals, symbols, and punctuation marks) that construct all or part of the signature.
- **Value:** Provide the value of the indicator
- **Description :**
  - Provide additional description as needed for indicators. This section will be used for DC3/DCISE only, so attribution information may be included.
  - Provide additional description as needed for indicators without attribution information so that it can be shared with others for situational awareness.
- **Are there additional indicators to report?** Select appropriate indicator (Network, Signature, Registry, Email, File, String, or None) and the appropriate page will be presented.

Registry Indicator Information (Supplemental)

- **Indicator Type:** Select Registry indicators.
- **Indicator Sub-Type:** Select one of the following Indicator types.
  - RegistryHive - Top level of registry; a section of the registry that appears as a file on your hard disk.
  - RegistryKeyPath - The complete path to the registry key.
  - RegistryKeyValue - This is the value contained within the defined registry key.
- **Value:** Provide the value of the indicator
- **Description :**
  - Provide additional description as needed for indicators. This section will be used for DC3/DCISE only, so attribution information may be included.
  - Provide additional description as needed for indicators without attribution information so that it can be shared with others for situational awareness.

- **Are there additional indicators to report?** Select appropriate indicator (Network, Signature, Registry, Email, File, String, or None) and the appropriate page will be presented.

Email Indicator Information (Supplemental)

- **Indicator Type:** Select Email indicators.
- **Indicator Sub-Type:** Select one of the following Indicator types.
  - Subject - This is the topic of the email content as indicated by the Subject field of the email message headers.
  - Sender - Purported originator of the message as indicated by the email address in the Sender field of the email message headers.
  - SenderIP - This is the Internet Protocol (IP) address of the device from which the message is purported to have originated.
  - Header - Information contained within the email message that is applied by the email client software and/or email servers through which the message is routed, and is typically not displayed to the user within email client software. Email headers may contain references to the type of software used to create or route the message, IP addresses and host names of devices through which the message is relayed, dates and times that messages traversed the device, etc.
  - EmailStringGeneral - Any string within the content of the email message that may be used to uniquely identify the message and does not meet the requirements of other indicator type.
  - SenderDisplayName - Common name of the purported originator of the email message as indicated by the Sender field of the email message headers.
  - DownstreamIPAddress - This is the Internet Protocol (IP) address of the device that last handled the email message prior to delivery to the intended recipient's email system.
  - Message-ID - A unique identifying string normally applied by the email server that first receives the email message from the originating email client. This string is typically in the format of [Unique String]@[Email Domain].
- **Value:** Provide the value of the indicator
- **Description :**
  - Provide additional description as needed for indicators. This section will be used for DC3/DCISE only, so attribution information may be included.
  - Provide additional description as needed for indicators without attribution information so that it can be shared with others for situational awareness.
- **Are there additional indicators to report?** Select appropriate indicator (Network, Signature, Registry, Email, File, String, or None) and the appropriate page will be presented.

File Indicator Information (Supplemental)

- **Indicator Type:** Select File indicators.
- **Indicator Sub-Type:** Select one of the following Indicator types.
  - FileAccessedTime - This is the time the file was accessed.
  - FileChangedTime - This is the time the file was changed.
  - FileCompileTime - This is the time the file was compiled

- FileCreatedTime - This is the time the file was created
- FileExtension - This is the file extension.
- FileFullPath - This is the full path for the file location.
- FileMD5 - This is the MD5 cryptographic hash value for the file.
- FileModifiedTime - This is the time the file was modified.
- FileName - This is the name of the file.
- FileOwner - This is the file owner as recorded by the file system.
- FileSize - This is the file size in bytes.
- FileStrings - A finite sequence of characters (i.e., letters, numerals, symbols, and punctuation marks) that define a particular file.
- FileSHA1 - This is the SHA1 cryptographic hash value for the file.
- FileSSDeep - A string that describes the SSDeep hash values for segments of the file.
- CompressionType - Details about the type of compression used or how the malware was packaged (if known).
- Malicious (Y/N) - Enter Y if the file was malicious and enter N if the file was not malicious (if known).
- MalwareType - The type of hostile, intrusive or otherwise malicious software or program code used in an incident (e.g. virus, worm, bot).
- MalwareFamily - The name given to a certain set of malware; usually occurs when malware becomes widespread and/or is identified by major AV companies. (e.g. Sober.A)

- **Value:** Provide the value of the indicator
- **Description :**
  - Provide additional description as needed for indicators. This section will be used for DC3/DCISE only, so attribution information may be included.
  - Provide additional description as needed for indicators without attribution information so that it can be shared with others for situational awareness.
- **Are there additional indicators to report?** Select appropriate indicator (Network, Signature, Registry, Email, File, String, or None) and the appropriate page will be presented.

String Indicator Information (Supplemental)

- **Indicator Type:** Select Signature indicators.
- **Indicator Sub-Type:** Select one of the following Indicator types.
  - AutonomousSystemNumber - The number assigned to an autonomous system on the Internet; an autonomous system consists of a collection of IP routing prefixes under the control of one or more network operators.
  - ATMAddress - Address used for endpoints in an Asynchronous ATM network.
  - MACAddress - Unique identifier assigned to most network interfaces or network cards.
  - UniformResourceLocator - An address that uniquely identifies a resource on the Internet.
  - ServiceName - The name of a service running on the system
  - Other

- **Value:** Provide the value of the indicator
- **Description :**
  - Provide additional description as needed for indicators. This section will be used for DC3/DCISE only, so attribution information may be included.
  - Provide additional description as needed for indicators without attribution information so that it can be shared with others for situational awareness.
- **Are there additional indicators to report?** Select appropriate indicator (Network, Signature, Registry, Email, File, String, or None) and the appropriate page will be presented.

Bulk Indicator Information (Supplemental)

- **Indicator Type:** Select Indicator Bulk Data.
- **Indicator Data:** List indicators in bulk CSV format in the text box provided. Use the following format in your submission: Indicator Type, Indicator Sub-Type, Indicator Value, Description – Private, Description- -Shared. This section is limited to 16,000 characters.
- **Are there additional indicators to report?** Select appropriate indicator (Network, Signature, Registry, Email, File, String, or None) and the appropriate page will be presented.

Indicators Only Summary Information

Section II: DIB Point of Contact

Note: If you are submitting an indicator only report, please provide Point of Contact information. If this is part of an initial report or follow-on report, this section is not repeated.

This section collects information for DC3/DCISE to contact the reporting partner regarding the reported incident. The DIB partner point of contact is a cleared individual identified and authorized to work directly with DC3/DCISE on cyber incident sharing and reporting. Enter the contact information of the individual that DC3/DCISE should contact regarding questions or feedback about the report.

- **Last name** - Enter the last name of the appropriate DIB partner point of contact.
- **First name** - Enter the first name of the appropriate DIB partner point of contact.
- **Email** - Enter the primary work email address of the appropriate DIB partner point of contact.
- **Company name** - Enter the name of the company that employs the DIB partner point of contact.
- **Location** - Enter the full postal mailing address for the work location of the DIB partner point of contact.
- **Phone** - Enter the daytime phone number of the appropriate DIB partner point of contact, including the country and area code (+x xxx-xxx-xxxx).
- **Fax** - Enter the daytime fax number of the appropriate DIB partner point of contact, including the country and area code (+x xxx-xxx-xxxx).
- **Division / group** - Enter the division or group in which the DIB partner point of contact works.
- **Time Zone** - Select the time zone in which the DIB partner point of contact resides.

- **Provide additional POC information as appropriate** (Click on POC link). If additional POCs are needed, select the appropriate category (incident response, technical or business unit points of contact). A new window will be presented to collect the additional POC information with the same fields as above.

Section II: Indicator Description

- **Incident Collection Form (ICF) number -** The DC3/DCISE will assign a unique identifier for tracking the incident report. The format of the identifier will be YYDDD-NNN, where YY equals the last two digits of the year, DDD is the day of the year, and NNN is the sequential report number (e.g., 10020-001). This number should be auto generated for a new report. For a follow-up report, enter the assigned DC3/DCISE number.
- **Do you require pre-publication review of the Customer Response Form (CRF)?** Following the submission of an ICF, DC3/DCISE will develop a customer response report as a means to provide analytical information back to the submitter. If the submitter would like to review the anonymized report before it is shared with other DIB Partners, select "Yes". The submitter will be provided the opportunity to review the report before it is released in final form to the entirety of the partnership. If no inputs are received within two federal business days from the time DC3/DCISE requests review, the lack of input will be logged, and the report published. If "No" is selected, the submitter will not be contacted for comments prior to release.
- **Description:**
  - Provide additional description as needed for indicators. This section will be used for DC3/DCISE only, so attribution information may be included.
  - Provide additional description as needed for indicators without attribution information so that it can be shared with others for situational awareness.
  - Select the type of indicators you would like to report. This will take you to the specific indicator reporting pages.
- **What type of indicators would you like to report?** Select the appropriate indicator (Network, Signature, Registry, Email, File, String, or Indicator block in CSV format) and the appropriate page will be presented.