GENERAL SERVICES ADMINISTRATION (GSA)
FEDERAL SYSTEMS INTEGRATION AND MANAGEMENT CENTER (FEDSIM)

REQUEST FOR INFORMATION (RFI)

IN SUPPORT OF THE
DEPARTMENT OF HOMELAND SECURITY (DHS)

NATIONAL SECURITY DEPLOYMENT (NSD)
CONTINUOUS DIAGONSTICS AND MITIGATION (CDM)

TO
ALLIANT SMALL BUSINESS HOLDERS

Issued: March 6, 2017

Responses Due: No later than 11:00am March 16, 2017

General Services Administration (GSA)
Federal Systems Integration and Management Center (FEDSIM)
Request for Information (RFI)
Alliant Small Business (ASB)

Disclaimer: This RFI does NOT constitute a Request for Proposal and is not to be construed as a commitment, implied or otherwise, by the Government that a procurement action will be issued. No telephone inquiries will be accepted and requests for solicitation packages will not be honored, as no solicitation is intended at this time. Response to this notice is not a request to be added to a bidders list or to receive a copy of a solicitation. No entitlement to payment of direct or indirect costs or charges by the Government will arise as a result of the submission of the requested information. No reimbursement will be made for any costs associated with providing information in response to this announcement and any follow up information requests. Responses to this RFI may be considered in the future determination of an appropriate acquisition strategy for the program. The Government may not respond to any specific questions or comments submitted in response to this RFI or information provided as a result of this request. Any information submitted by respondents as a result of this notice is strictly voluntary.

I. Introduction to Alliant Small Business (ASB) GWAC Contract Holders

General Services Administration (GSA) FEDSIM is releasing this Request for Information (RFI) on behalf of the Department of Homeland Security, National Protection and Programs Directorate, (NPPD)/Office of Cybersecurity and Communications (CS&C)/Network Security Deployment (NSD). The purpose of this RFI is to assist the Government in conducting market research focused on identifying GSA Alliant Small Business (ASB) GWAC contract holders that may have the capability and expertise to support the scope of requirements described below for Continuous Diagnostics and Mitigation (CDM) support to civilian U.S. Government agencies. This information will be used for market research only. The Government is not obligated to release a future solicitation.

II. Background

Strengthening the security posture of Federal networks, systems and data is one of the most important challenges we face as a nation. As such, the General Services Administration (GSA) and the Department of Homeland Security (DHS) have partnered to provide customer agencies with a Continuous Diagnostics and Mitigation (CDM) Program to safeguard, secure and strengthen cyberspace and the security posture of Federal networks in an environment where the cyberattack threat is continuously growing and evolving.

The CDM Program is a federally-funded program designed to provide a new approach to protecting the cyber infrastructure of the civilian .gov network environment. The CDM Program moves away from historical compliance reporting toward combating threats to our nation's networks on a real-time basis, where tools are gathering system attributes to determine the current state of the network.

The scope of the CDM program is defined by managing:

- "What is on the network?"
- "Who is on the network?"
- "What is happening on the network?"
- "How is the network protected?"
- "What data is on the network"

The CDM Program offers all state, local, regional, tribal and federal agencies, the ability to enhance and further automate existing continuous network monitoring capabilities, correlate and analyze critical security-related information, and enhance risk-based decision making at the agency and Federal enterprise level, consistent with Office of Management and Budget Memo 14-03 "Enhancing the Security of Federal Information and Information Systems," November 18, 2013.

In August 2013, GSA FEDSIM, working with DHS, awarded the CDM Tools/Continuous Monitoring as a Service (CMaaS) Blanket Purchase Agreement (BPA) under GSA IT Schedule 70, to support DHS in implementing the CDM Program. The CMaaS BPA is the mechanism by which agencies can access the tools, sensors and integration services that have been found technically acceptable under the CDM program.

The following table summarizes the current CDM Orders and the corresponding agencies supported by each:

Task Order	Contract Vehicle	Agencies Supported
TO2A	CMaaS BPA	DHS
TO2B	CMaaS BPA	DOE, DOI, DOT, EOP, USDA, VA, OPM
TO2C	CMaaS BPA	DOC, DOJ, DOL, State, USAID

TO2D	CMaaS BPA	GSA, HHS, NASA, SSA, Treasury, USPS
TO2E	CMaaS BPA	Education, EPA, HUD, NRC, NSF, SBA
TO2F	Alliant GWAC and CMaaS BPA for products	41 non-CFO Act agencies
PRIVMGMT	CMaaS BPA	65 agencies
CREDMGMT	CMaaS BPA	26 agencies

It is the intent that the Agency Groupings (TO2A-F) above would be preserved in the execution of future acquisitions within the scope of this RFI.

III. Scope

Specifically, the scope of services for which this RFI is seeking information includes:

a. Maintain and operate the existing CDM Solution to ensure a common set of CDM capabilities across all installations

b. Plan, provision, configure, operate, test, and manage tools, sensors, data feeds and dashboard integration as part of the solution.

c. Integrate, operate, and maintain the Agency level CDM Dashboard

d. Develop and maintain the capability for CDM tools and sensors to report information to the Agency Dashboard

e. Refresh and integrate enhanced CDM capabilities, while ensuring continued operation of the functioning CDM solution

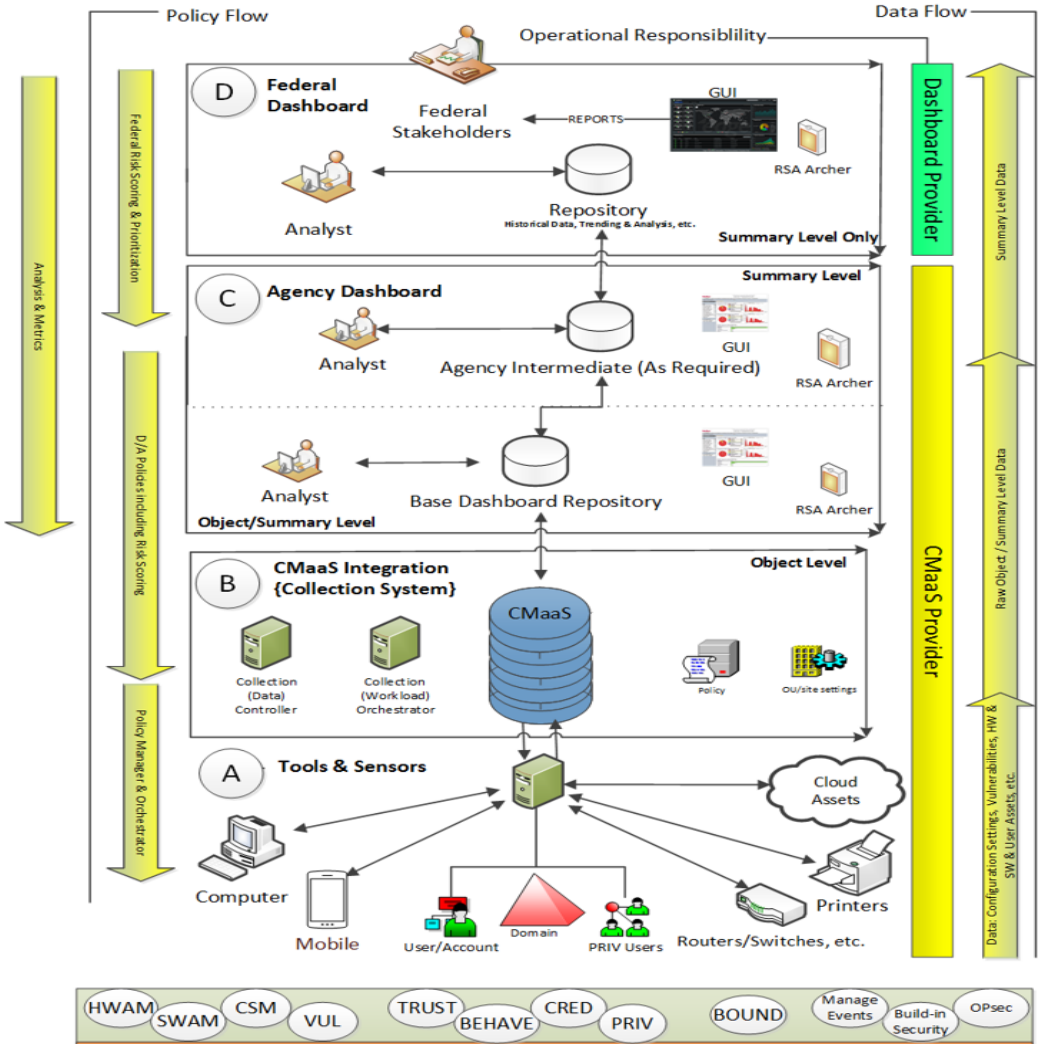
f. Design, build, deploy, and operate CDM Solution for new agencies that opt-in to the CDM Program

g. Provide Agency-specific training for the CDM Solution with an emphasis on introductory level operation and maintenance of the implemented tools and technologies, the Agency CDM Dashboard, and support for Information Security

Continuous Monitoring and CDM governance frameworks and processes consistent with the office of Management and Budget (OMB) and other federal oversight entities.

The CDM architecture is as follows:

- Area A is the location for tools and sensors that, together, provide the coverage of the CDM Tool Functional Areas.
- Area B is the integration point solution that supports the required integration and operational control points for the CDM Solution.
- Area C is the D/A CDM Dashboard(s) that integrates into the D/A CDM Solution.
- Area D is the Federal CDM Dashboard. As such, this area has no contractor responsibilities and is being provided by a separate CDM Dashboard TO.



IV. CDM Areas

The purpose of this RFI is to assist the Government in conducting market research focused on identifying GSA Alliant Small Business (ASB) GWAC contract holders that may have the capability and expertise to provide the scope of services to the following CDM capability areas to the participating civilian U.S. Government agencies:

Manage what is on the network. Encompass activities that identify the existence of hardware infrastructure devices, the accurate identification of approved software components, verification and validation that devices have the correct security configuration settings, and hardening the system platform to reduce the platform attack surface.

The CDM Solution may require expansion of "What is on the Network" capabilities to Cloud and Mobile assets (see Area A of the CDM Notional Architecture diagram above). Cloud and Mobile assets are defined as:

a) *Cloud Assets* - As defined in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-145, "cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." The nature of the dynamics for shared resources provides challenges to the timing windows within traditional asset tracking. The CDM Program requires the ability to identify the connection mechanism to Cloud Service Provider service data source and the establishment of the work flow to provide this information ultimately to the CDM Dashboard.

b) *Mobile Assets* - As defined in NIST SP 800-124 Rev 1, "The following hardware and software characteristics collectively define the baseline of mobile devices:
    i. A small form factor.
    ii. At least one wireless network interface for network access (data communications). This interface uses Wi-Fi, cellular networking, or other technologies that connect the mobile device to network infrastructures with connectivity to the Internet or other data networks.
    iii. Local built-in (non-removable) data storage.
    iv. An operating system that is not a full-fledged desktop or laptop operating system.
    v. Applications available through multiple methods (provided with the mobile device, accessed through web browser, acquired and installed from third parties)."

Manage who is on the network. Encompass activities that identify and determine user privileges, credentials, and systems with access authorization, authenticated permissions and granted resource rights.

Manage what is happening on the network. Encompass activities that would include the following:

a) Incident Response Automation. From the CDM capabilities point of view, the incident response function can be viewed as two distinct functions. In the first capability, there are functions that are necessary to report the incident response

reporting for inclusion in the Agency Dashboard. In the second, there is the orchestration that is necessary to support the respond function with automated tools to the extent possible.

The reporting function consists of providing the audit and logging infrastructure that will allow for the collection and logging of events related to the detection of incidents. This capability is focused on the detection of security events within the Agency infrastructure and is an indication of the effectiveness of the controls that were put in place to prevent such intrusions. The incident response monitoring capability also includes the orchestration necessary to collect these types of logging and correlating them for reporting to the Agency Dashboard.

The second capability, orchestration to support the respond function, is focused on providing the following capabilities:

- Incident Response Event Notification
- Incident Handling Data Collection
- Incident Monitoring
- Incident Reporting
- Incident Response Devices

This area also includes development and refinement of processes and procedures to prioritize incidents and associated response actions, to quickly mitigate the impact of an incident, take appropriate remediation actions to eliminate the impact (restore normal operations) of the same incident, and to support information sharing and collaboration (both internal and external) to minimize or prevent the impact of future incidents.

b) Ongoing Assessment and Authorization. The Federal government has a need to improve the efficiency, data quality and currency, and reduce cost related to current security assessment & authorization processes. The Federal government requires a capability to help increase greater automation, accuracy and currency related to the implementation status of Agency NIST 800-53r4 controls and their Agency-defined parameters. This capability would also be able to uses the results of the ongoing assessment of NIST SP 800-53 controls for all previous phases of CDM as a set of inputs for the orchestration of ongoing authorization and risk assessment and acceptance processes.

Manage how the network is protected. Encompass activities that would include the following:

a) Bound Filtering by Network. The BOUND function provides Agency visibility into the risk associated with connections or access to networks, systems and data. Manage Network Filters and Boundary Controls (BOUND-F) network filters include devices such as firewalls and gateways that sit at the boundary between enclaves (such as a trusted internal network or subnet, and an external or internal, less-trusted network). The filters apply sets of rules and heuristics to regulate the flow of traffic between the trusted and less trusted sides based on network attributes (such as ports and protocols). The overall purpose of BOUND-F is to reduce the probability that unauthorized traffic passes through a network boundary.

b) Bound Filtering by Content. Content Based Perimeter Protection focuses on the prevention of unwanted content from entering or leaving the gateway of a network. Content filtering examines network traffic at the application level to block or filter malware or prohibited traffic from entering or leaving the network. The two common areas of content filtering are web (HTTP) and email (SMTP).

c) Data Based Perimeter Protection. The data based perimeter protection is a broad category of protections that include the technologies used for Data Leak/Loss Prevention (DLP). The objective of this protection is to provide the capability to mitigate the effects of insider threat activities to include such aspects as:

- Unauthorized file manipulation
- Printing protected data
- Exporting protected data outside of the Agency
- The ability to intercept protected data as it transits the Agency network

d) Bound Encryption (Bound-E). Cryptographic mechanisms are used to protect credentials, data at rest, and data in motion. An identity credential is a digital representation of a user. The identity credentials are often implemented on an integrated circuit smart card, in particular the Federal personal identity verification (PIV) card with which is specified in FIPS-201-2. FIPS 201 credentials commonly include information such as private keys, pins, digital certificates, and encoded biometric values. Credentials are used to authenticate users, systems, software packages and other resources in the system. Data at rest protection includes encryption of individual files, as well as encryption of entire volumes/disks.

Components of data at rest encryption include both the encryption software itself and the encrypted data. Data in motion cryptography involves the use of application security protocols such as S/MIME and SSH; web-based transactions using SSL/TLS; and VPNs using IPsec and SSL/TLS.

Together these cryptographic techniques and related cryptographic keys/credentials provide critical security functions to support the confidentiality, integrity and authenticity of network functions both internally to protect insider threats and externally to prevent malicious behaviors.

e) System Assurance (Software/Hardware). The goals of system assurance are to reduce the attack surface for network and infrastructure components during acquisition, development, and deployment, to ensure the provision of the least vulnerable solutions to Agencies, and to reduce project costs associated with addressing security vulnerabilities and weaknesses in fielded systems due to insertion of counterfeits, unauthorized production, tampering, theft, insertion of malicious software and hardware, as well as poor manufacturing, development, and poor security engineering practices. The following capabilities support this goal:

- Supply Chain Risk attributes
- Software development assurance (code inspection/analysis to remove weaknesses and vulnerabilities from the software)
- Application weakness detection (Web-based vulnerabilities such as Common Weakness Enumeration and secure configuration, as well as Database focused)

f) Cyber Incident Surge Support. Cyber incident surge support may be required on an emergency basis in the event participating Agencies in the TO are impacted by cyber-attacks. The scope of the response may include an initial assessment of the attack, identifying a plan of action, and implementing the approved response action.

Additional activities may encompass the following:

a) Micro-segmentation is the virtualization of the data center or a cloud computing structure. It is a security technique that integrates security directly into the virtualized workload and eliminates the requirement of hardware based firewalls. One of the characteristics of micro-segmentation is that it is persistent. With micro-segmentation, security policies can be placed on the virtual connections that can

move with an application if the network is reconfigured. This makes security on the network persistent as well as ubiquitous. Hence, micro-segmentation enhances the current and future security posture of a network.

b) Enterprise digital rights management, also commonly referred to as information rights management, provides persistent protection of information regardless of its transience within or external to the enterprise. The DRM tool can be facilitated by a combination of onsite or offsite technology presence (e.g. cloud provided) and should provide sufficient protection mechanisms such that unauthorized access to the data is prevented through strong technical means (e.g. encryption of data) which is capable of being centrally managed by the enterprise. DRM tools should provide some level of assurance that loss of the digital artifacts to an untrusted agent do not necessarily result in the loss of the data contained within.

c) Advanced Data Protection is the process of safeguarding important information from corruption, loss, or exposure to unintended recipients. The term Advanced data protection is used to describe both operational considerations such as backup of data and disaster recovery/business continuity as well as information security considerations such as data classification, access controls, data transformation, and monitoring and auditing.

V. Instructions to Respondents

Respondents to this RFI should be aware that the Government is seeking respondents who can demonstrate their ability to meet the scope and requirements of the CDM effort described within DHS CDM requirements of this RFI.

Specifically, interested respondents are requested to complete a Questionnaire, provide a Corporate Capabilities Package, and provide Corporate Experience Sheets in order for the Government to conduct an initial review of market capabilities.

a. Questionnaire, Attachment A

Interested respondents are requested to provide information using the attached Questionnaire.

b. Corporate Supply Chain Risk Management (SCRM) Capabilities, Attachment B

Respondents shall complete the Corporate SCRM Capabilities Sheet for its corporate capability and experience with SCRM.

c. Corporate Capabilities, Attachment C

The Government requests all respondents to submit a Corporate Capabilities Package to better define what your corporation is, who it serves, what services it provides, and how it ensures quality delivery. The Corporate Capabilities Package should include a description of the processes, procedures, and practices used to assure the integrity, security, resilience, and quality of the offered services. Corporate Capabilities will be considered against current needs and services as required by the Government for the DHS CDM effort described within this RFI.

d. Corporate Experience, Attachment D

Respondents shall complete Corporate Experience Sheets for its past performance from contracts in the last three years in which the interested respondent (as a prime contractor or subcontractor) provided services similar in complexity and scope to the requirements identified in this RFI. Interested respondents should ensure that all of the points of contact are aware that they may be contacted.

e. RFI Responses

All responses MUST be submitted electronically with 'DHS CDM RFI' and the responding Company/Firm's name in the subject line directly to the FEDSIM Contracting Officer (CO) and Contract Specialist (CS) no later than (NLT) 11AM EST on **Monday March 16, 2017** directly to the following email addresses:

John Terrell, CO: john.terrell@gsa.gov
Johnny Montgomery, CS: johnny.montgomery@gsa.gov

No phone calls will be accepted. Please DO NOT send responses in a PDF format/file. The responses shall be concise and **shall not exceed twelve pages**, have no smaller than Times New Roman12 point font size, and have one inch margins all around. There is no font size restriction for graphics. Cells in the Corporate Experience table in Attachment 2 may be stretched as needed to fit required information, subject to the overall page limitation. Any additional capability statements, white paper or other brochure materials **should not** be provided.

The twelve pages should include the following:

- Cover Page
- Questionnaire
- Corporate SCRM Capabilities
- Corporate Capabilities Package
- Corporate Experience. All corporate experience should reflect scope relevant to this acquisition.

Any comments, concerns, and/or questions regarding this requirement must be emailed to the CO at john.terrell@gsa.gov and CS at johnny.montgomery@gsa.gov at least three Government work days prior to the RFI due date identified above with CDM RFI and the responding Company/Firm's Name in the subject line.

f. Disclaimer

This RFI neither constitutes a solicitation, Request for Proposal (RFP), Invitation for Bid, or promise to issue an RFP in the future, nor does it restrict the U.S. Government to an ultimate acquisition approach. This RFI is issued solely for information and planning purposes and should not be construed as a commitment by the Government for any purpose.

All interested parties are encouraged to respond fully to this RFI. Respondents are advised that the Government will not pay for any information or administrative costs incurred in response to this RFI; all costs associated with responding to this RFI will be solely at the interested parties' expense. All submissions become Government property and will not be returned.

The Government is in no way obligated by the information received and all information submitted by respondents to this RFI is strictly voluntary. Respondents who submit information in response to this RFI do so with the understanding that Government personnel, as well as their support Contractors, may review their material and/or data.

Not responding to this RFI does not preclude participation in any future procurement, if any is issued. However, the Government places tremendous value on the information received and will utilize it to implement and finalize its acquisition strategy.

Sincerely,

\\ s\\

John Terrell
Contracting Officer
FEDSIM Acquisition

Enclosures:
A - Corporate Overview
B - Corporate SCRM Capabilities
C - Corporate Capability Statements
D - Corporate Experience

Attachment A
Corporate Overview

Description and definition of some items are provided below the table.

Name of Company/Firm	
Name of Business Unit Responding to the RFI (if applicable)	
Alliant Small Business Contract Number:	
Designated Point of Contact (provide one) **Name** **Phone Number** **Email Address**	
DUNS Number	
Corporate Address	
Total Number of Full-Time Employees	
Total Number of Full-Time Consultants	
Date of Establishment	
Corporate Website URL	
Business Classification	
Is the Company/Firm under NAICS Code(s) 541412 Small Business? (Yes/No)	

Provide additional Socioeconomic designation of small business contractor (if applicable) – Woman-Owned, Service Disabled Veteran Owned, HUBZone	
Does the Company/Firm currently possess a cost accounting system deemed adequate by a cognizant audit agency (e.g., DCAA Approved)? (Yes/No) **Name the audit agency.**	
Does the Company/Firm currently possess a Government approved purchasing system? (Yes/No)	
Please indicate if forward pricing rates have been established with DCAA or DCMA for direct and indirect rates. If your firm is a joint venture (JV), indicate if the rates were established for the JV, or individual member(s). If rates are established for member(s) and not the JV itself, indicate how you intend to apply the rates on the JV.	
Please indicate the date of your firm's most recent DCAA or DCMA approved provisional billing rates. If your firm is a JV, indicate if the rates were established for the JV, or individual member(s). If rates are established for member(s) and not the JV itself, indicate how you intend to apply the rates on the JV.	
Does the Company/Firm have an Insider Threat Program? Indicate whether the Program is NISPOM, CDM or Other (see below this table for description).	
Does the Company/Firm participate as an Information Sharing and Analysis Organization (ISAO) Member (see below)? (Yes/No)	
Does the Company/Firm participate in Automated Indicator Sharing (AIS)? (Yes/No)	

Is the Company/Firm enrolled in Enhanced Cybersecurity Services (ECS)? (Yes/No)	
Is the Company/Firm a participant in the Cyber Information Sharing and Collaboration Program (CISCP)? (Yes/No)	
Does the Company/Firm utilize the Cyber Security Evaluation Tool (CSET)? (Yes/No)	
Does the Company/Firm implement the NIST Cybersecurity Framework? (Yes/No)	
Does the Company/Firm implement NIST Special Publication 800-171 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations? (Yes/No)	
Indicate whether the Company/Firm Federal Risk and Authorization Management Program (FedRAMP) compliant and possess a FedRAMP Authority to Operate (ATO) – or - has corporate experience obtaining a FedRAMP ATO.	
Is the Company/Firm compliant with Earned Value Management System (EVMS) American National Standards Institute/Electronic Industries Alliance (ANSI/EIA) standard 748? (Yes/No)	
Is the Company/Firm compliant with International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27036 – Information Security Management? (Yes/No)	

Is the Company/Firm compliant with ISO/IEC 27036 – Information Security Management – Security Techniques – Information Security for Supplier Relationships? (Yes/No)	
Is the Company/Firm a participant in the Customs-Trade Partnership Against Terrorism (C-TPAT)? (Yes/No)	

Insider Threat Program (ITP)
An Insider Threat is defined as a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and is a risk to intentionally misuse that access to negatively affect the confidentiality, integrity, or availability of the organization's information or information systems.

National Industrial Security Program Operating Manual (NISPOM) ITP
Contractors that hold a current Facility Clearance and an ITP that complies with the NISPOM; and the ITP covers the business unit that is providing products or services to the CDM program, shall be considered to have met the CDM Insider Threat program requirements. Requirements for establishing a NISPOM ITP are outlined in paragraph 1-202, DoD 5220.22-M Change 2 of the NISPOM, with additional guidance provided in Industrial Security Letter (ISL) 2016-02 and the Defense Security Service (DSS) Process Manual for the Certification and Accreditation of Classified Systems under the NISPOM Change 2, Version 3.3 May 2016 for the Certification and Accreditation of Classified Systems under the NISPOM. Additional guidance on establishing a NISPOM-compliant ITP is available in the Center for Development of Security Excellence Insider Threat Toolkit, available at: http://www.cdse.edu/toolkits/insider/index.php, and in the Carnegie Mellon University Software Engineering Institute (SEI) Common Sense Guide to Mitigating Insider Threats, available at: http://www.cert.org/insider-threat/best-practices/index.cfm.

CDM ITP
Requirements for the CDM ITP are modeled after the National Insider Threat Policy for cleared industry, as outlined in the NISPOM (see above). Contractors that do not have a current ITP that complies with the NISPOM can meet the CDM Insider Threat Program requirements by achieving the following minimum requirements:

- Establish an Insider Threat Program and self-certify the Implementation Plan in writing to the CDM program;
- Provide Insider Threat training for Insider Threat Program personnel and awareness for

other employees;
- Monitor network activity;
- Gather, integrate, and provide for reporting of relevant and credible information indicative of a potential or actual insider threat to deter employees from becoming insider threats; detecting insiders who pose a risk to Federal information obtained in the course of performing work for the CDM Program; and mitigating the risk of an insider threat; and
- Conduct self-inspections of Insider Threat Program.

Other ITP
An insider threat program or other means of addressing insider threats that does not meet the requirements of either a NISPOM or CDM ITP as described above.

Information Sharing and Analysis Organization (ISAO) Membership
Information sharing is essential to furthering cybersecurity for the nation. As the lead federal department for the furthering of cybersecurity, DHS has developed and implemented numerous information sharing programs. Through these programs, DHS develops partnerships and shares substantive information with the private sector, state, local, tribal, and territorial governments and with international partners, as cybersecurity threat actors are not constrained by geographic boundaries. Information about the DHS information sharing programs listed in this section is available at: https://preview.dhs.gov/topic/cybersecurity-information-sharing.

An ISAO is a group created to gather, analyze, and disseminate cyber threat information. ISAOs offer a flexible approach to self-organized information sharing activities amongst communities of interest such as small businesses across sectors: legal, accounting, and consulting firms that support cross-sector clients, etc. Organizations engaged in information sharing related to cybersecurity risks and incidents play an invaluable role in the collective cybersecurity of the United States.

Automated Indicator Sharing (AIS)
AIS is a free capability that enables the exchange of cyber threat indicators between the Federal Government and the private sector at machine speed. Threat indicators are pieces of information like malicious IP addresses or the sender address of a phishing email (although they can also be much more complicated). AIS is a part of the DHS effort to create an ecosystem where as soon as a company or federal agency observes an attempted compromise, the indicator will be shared in real time with all of our partners, protecting them from that particular threat.

Enhanced Cybersecurity Services (ECS)
The ECS program is an intrusion prevention capability that helps U.S.-based companies protect their computer systems against unauthorized access, exploitation, and data exfiltration. ECS works by sharing sensitive and classified cyber threat information with accredited Commercial Service Providers (CSPs). These CSPs in turn use that information to block certain types of

malicious traffic from entering customer networks.

Cyber Information Sharing and Collaboration Program (CISCP)
CISCP is DHS's flagship program for public-private information sharing. Information shared via CISCP allows all participants to better secure their own networks and helps support the shared security of CISCP partners. Further, CISCP provides a collaborative environment where analysts learn from each other to better understand emerging cybersecurity risks and effective defenses. CISCP is based upon a community of trust in which all participants seek mutual benefit from robust information sharing and collaboration. CISCP is free of charge and provides value to all members. Therefore, all companies with an interest in multi-directional cybersecurity information sharing and robust analytic collaboration between the government and the private sector should consider joining CISCP.

Cyber Security Evaluation Tool (CSET)
The Cyber Security Evaluation Tool (CSET®) is a DHS product that provides users with a systematic and repeatable approach for assessing the security posture of their cyber systems and networks.

National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)
The NIST CSF can be used to align cybersecurity decisions to mission objectives; organize security requirements originating from legislation, regulation, policy, and industry best practice; communicate cybersecurity requirements with stakeholders, including partners and suppliers; integrate privacy and civil liberties risk management into cybersecurity activities; measure current state and express desired state; prioritize cybersecurity resources and activities; and analyze trade-offs between expenditure and risk.

NIST Special Publication 800-171 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
The protection of Controlled Unclassified Information (CUI) resident in nonfederal systems and organizations is of paramount importance to federal agencies and can directly impact the ability of the federal government to successfully conduct its assigned missions and business operations. The security requirements of Special Publication 800-171 apply to all components of nonfederal systems and organizations that process, store, or transmit CUI, or that provide security protection for such components.

Federal Risk and Authorization Management Program (FedRAMP) Authority to Operate (ATO)
FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. FedRAMP authorizes cloud systems through security assessments, leveraging and authorization, and ongoing assessment and authorization. Compliant cloud solutions are granted a FedRAMP ATO.

EVMS ANSI/EIA Standard 748
EVMS ANSI/EIA Standard-748 incorporates best business practices for program management systems that have been proven to provide strong benefits for program and enterprise planning and control. Additionally, industry standards often require compliance with the ANSI standard as part of project management best practices.

ISO/IEC 27001 – Information Security Management
The ISO/IEC 27000 family of standards helps organizations keep information assets secure. Using this family of standards will help your organization manage the security of assets such as financial information, intellectual property, employee details or information entrusted to you by third parties.

ISO/IEC 27036 – Information technology -- Security techniques -- Information Security for Supplier Relationships
ISO/IEC 27036 provides guidance to assist organizations in securing their information and information systems within the context of supplier relationships.

C-TPAT: Customs-Trade Partnership Against Terrorism
When an entity joins C-TPAT, an agreement is made to work with U.S. Customs and Border Protection to protect the supply chain, identify security gaps, and implement specific security measures and best practices. Applicants must address a broad range of security topics and present security profiles that list action plans to align security throughout the supply chain. C-TPAT members are considered to be of low risk, and are therefore less likely to be examined at a U.S. port of entry.

Attachment B
Corporate Supply Chain Risk Management (SCRM) Capabilities

CRITERIA	YES/NO
Original Manufacturer Purchasing	

Original Manufacturer Purchasing
Ensuring that the goods provided to the government are authentic and have not been altered or tampered with is an important step in mitigating supply chain risk. Inauthentic components often do not have the latest security-related updates or are not built to the original equipment (or component) manufacturer's (OEMs) security standards. The risk of receiving inauthentic, counterfeit, or otherwise nonconforming items is best mitigated for the CDM program by obtaining required components and end items only from OEMs, their authorized resellers, or other trusted sources.

Provide information regarding whether the corporation has a documented policy and methods to:

- First obtain electronic parts that are in production by the original manufacturer or an authorized aftermarket manufacturer or currently available in stock from
    - The original manufacturers of the parts;
    - Their authorized suppliers, which is a supplier, distributor, or an aftermarket manufacturer with a contractual arrangement with, or the express written authority of, the original manufacturer or current design activity to buy, stock, repackage, sell, or distribute the part.; or
    - Suppliers that obtain such parts exclusively from the original manufacturers of the parts or their authorized suppliers
- Qualify any non-OEM or non-authorized source so that by the source, the security and the integrity of the item being purchased is guaranteed
- Validate and test end items from non-OEM or non-authorized sources
- Conduct reviews and approvals of sources to qualify third party sources
- Enforce terms and conditions for purchases made from non-OEM or non-authorized sources

Attachment B:

Corporate Capability Statements

All interested respondents are requested to provide the following information:

- Describe your company's profile and core capabilities.
- Do you propose to submit as a prime should a solicitation result from this market research?
- Complete the corporate capability matrix below with a yes or no response. For every 'yes' response, address that area in the corporate capability statement.
- Describe your corporate capabilities as they relate to an integrated holistic approach for the following:
    a. Describe your corporate capabilities to design, install, configure and customize, test, and then operate a cybersecurity solution in highly complex environments.
    b. In addition, address your corporate capability to provide cybersecurity specific governance and technical training support tailored to different entities.

CDM Area	**Corporate Capability (Yes/No)**
Manage what is on the network	
Cloud Assets	
Mobile Assets	
Manage who is on the network	
Manage what is happening on the network	
Incident Response Automation	
Ongoing Assessment and Authorization	
Bound Filtering by Network	

Bound Filtering by Content	
Data Based Perimeter Protection	
Bound Encryption (Bound-E)	
System Assurance (Software/Hardware)	Supply Chain Risk attributes: Software Development Assurance: Application Weakness Detection:
Cyber Incident Surge Support	
Micro-segmentation	
Enterprise digital rights management	
Advanced Data Protection	

Attachment C
Corporate Experience

Please provide up to **three examples** of the ASB Prime's corporate experience (not required to have been provided through the ASB GWAC) as they relate to the CDM Program.

Program or Task Order Title		
Is/did the Company/Firm perform work as a Prime or Subcontractor?		
Percent of Work Performed by the Company/Firm		
Customer Name		
Customer Address	Street:	
	City, State:	Zip Code:
Phone Number:		
Contract Points of Contact:		
Contractual	Technical	
Name	Name	
Title	Title	
Organization	Organization	
Address	Address	
Phone	Phone	
Email	Email	
Contract Type	Contract Value	
Contract Number	Period of Performance	

If Award Fee - % of Fee Received		
Program Description (Size, scope, requirements, complexity as related to the RFI)	IT systems supported: (hardware/software configuration)	
How is this project related to the effort identified in the RFI?		
Major Deliverables:	Project Start Date	
	Original Completion Date	
	Estimated/Actual Completion Date	
	Explanation of Delay (If applicable)	
Problems encountered and solutions provided:	Original Value	
	Current Value	
	Estimated/Actual Completion Date	
	Explanation of Cost Growth (If applicable)	