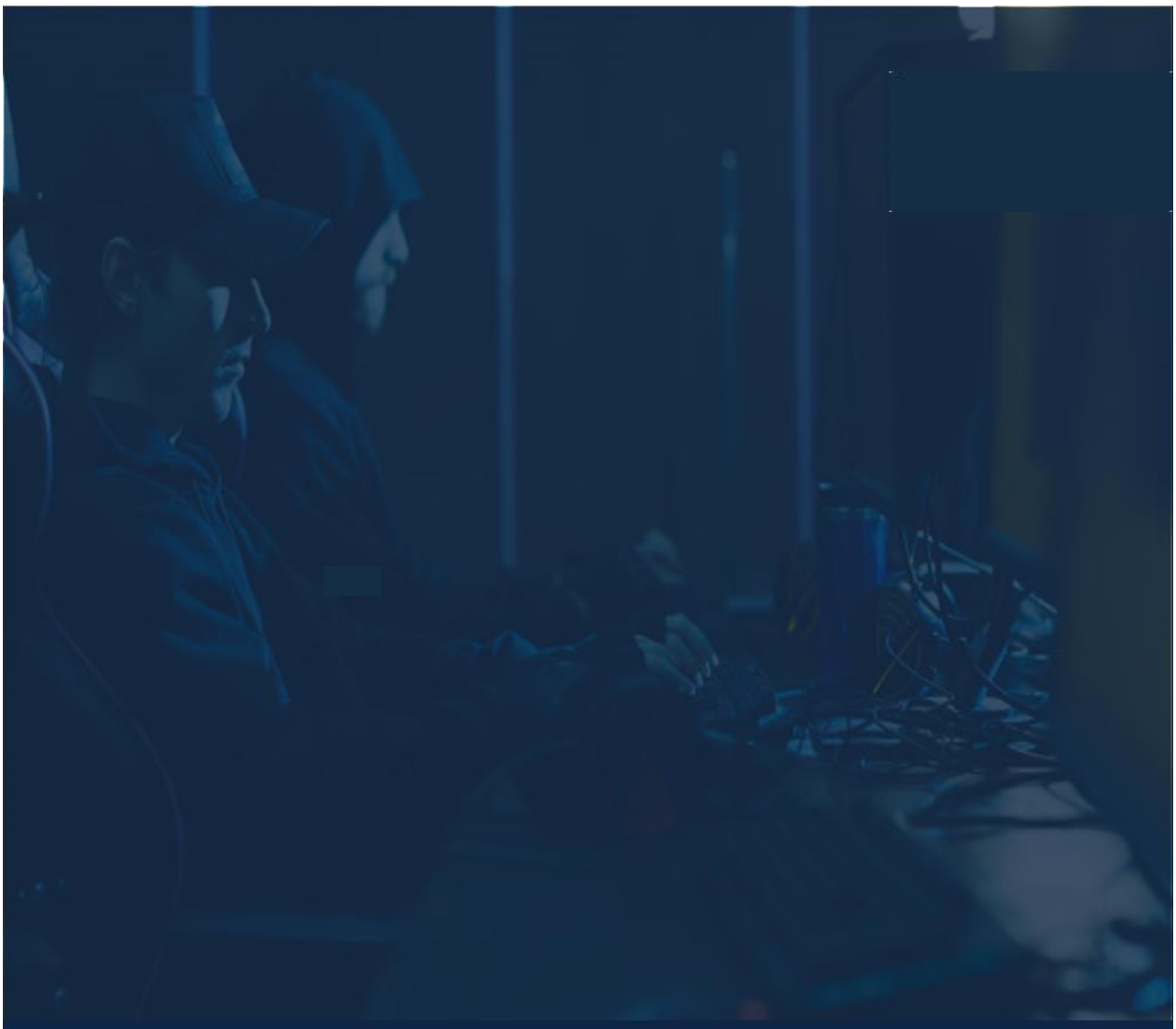


Advanced Persistent Threat (APT)

Buyer's Guide

GSA July 2022 Version 2.0

Executive Summary

In 2010, the Google Aurora attack forever changed the way organizations look at internet security. This large-scale, sophisticated attack demonstrated to all sectors, from public to private, that they are vulnerable to a new class of security breach, the Advanced Persistent Threat (APT). Once limited to opportunistic criminals, cyber-attacks are becoming a key weapon of state sponsored entities seeking to exert increased influence, defend national sovereignty and project national power.

More recently, the SolarWinds compromise brought to light the enormous third-party vendor risk to one's supply chain. This compromise, and others like it, has demonstrated that APTs leverage highly sophisticated Tactics, Techniques, and Procedures (TTPs), which can only be successfully countered by a well-trained, proven organization; an organization equipped with specialized knowledge and skill to identify, protect, and detect APTs comprehensively and to adequately respond and recover.

Awareness and preparation are fundamental elements in cybersecurity planning and the management of risks. Because each organization's risks, priorities, and systems are unique, the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) can be used as a planning tool to help organizations prioritize opportunities for improvement within the context of a continuous and repeatable process in cybersecurity functions: Identify, Protect, Detect, Respond, and Recover. As such, organizations well versed in applying the principles of the CSF are better prepared to handle APTs with a well-trained and prepared response.

This buyer's guide provides key considerations organizations can utilize in the evaluation of a potential APT product, solution, or service. Ultimately, the guide will provide a mechanism for organizations to engage capable, proven industry partners to deal with APTs to enhance the overall resilience of the Nation's cybersecurity posture.

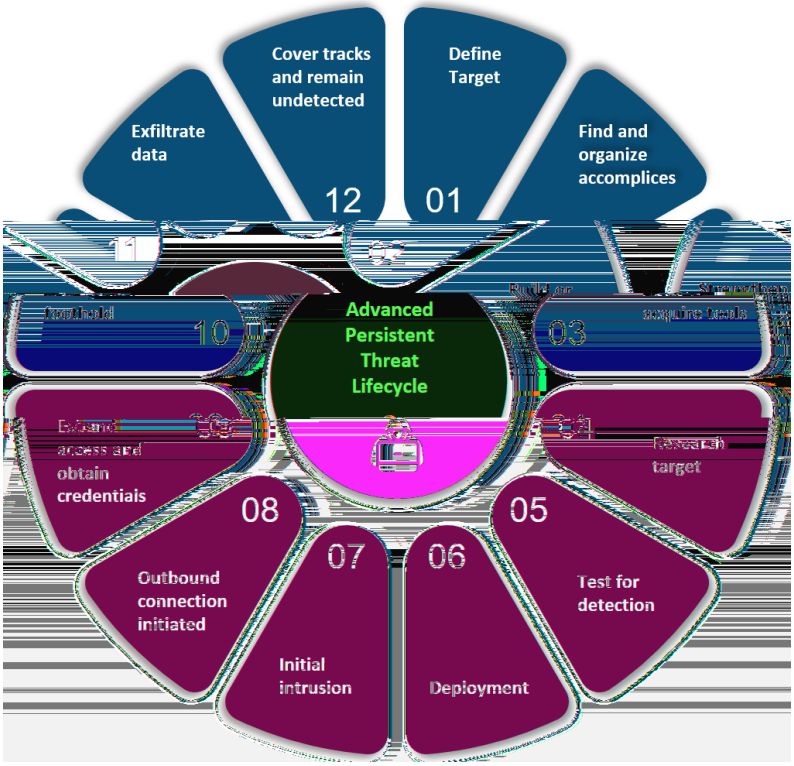
What are Advanced Persistent Threats?

An APT refers to a continuous computer hacking process in which a cybercriminal carries out a prolonged attack against a specific target. An APT is no run-of-the-mill cybersecurity hazard. APTs are long-term operations designed to infiltrate and/or exfiltrate as much valuable data as possible without being discovered. An APT can last for many months and can-do untold damage to an enterprise in stolen data and trade secrets.

Advanced Persistent Threat Lifecycle

As APTs grew in number, they also evolved and matured. APTs take advantage of multiple attack points in systems and networks and hijacking users' credentials at a low and slow pace to remain inconspicuous and undetected. Consequently, the lifecycle of an APT is much longer and

more complex than other kinds of attacks. The illustration below highlights the autonomy of a typical APT attack.



Advanced Persistent Threats Groups

APT groups are widely classified as organizations that lead attacks on a country's information assets of national security or strategic economic importance through either cyber espionage or cyber sabotage. They are more elusive, sophisticated, and effective at what they do than traditional hackers.

Threat actors who lead APT attacks tend to be motivated and committed. They have a goal in mind and are organized, capable, and intent on carrying out that goal. Some of these threat actors exist under a larger organization, like a nation-state or corporation.

These groups are engaged in espionage with the sole purpose of gathering intelligence or undermining the target's capabilities.

Some examples of well-known APT groups that target the U.S. Government include:

- **APT29**

  Also known as: Cozy Bear

Suspected attribution: Russia/Eastern Europe, these cyber-attacks are more technically advanced and highly effective at evading detection.

Sponsor: State-sponsored

Target sectors: Western and European governments, foreign policy groups and other similar organizations

Motivation: Information theft and espionage

Overview: APT29 is an adaptive and disciplined threat group that hides its activity on a victim's network, communicating infrequently and in a way that closely resembles legitimate traffic. By using legitimate popular web services, the group can also take advantage of encrypted SSL connections, making detection even more difficult. APT29 is one of the most evolved and capable threat groups. It deploys new backdoors to fix its own bugs and add features. It monitors network defender activity to maintain control over systems. APT29 uses only compromised servers for Command and Control (CnC) communication. APT29 counters attempts to remediate attacks. It also maintains a fast development cycle for its malware, quickly altering tools to hinder detection.

Associated malware: SUNBURST, HAMMERTOSS, TDISCOVER, UPLOADER

Best Known Compromise: SolarWinds (2020)

Attack vectors: APT29 has used social media sites such as Twitter or GitHub, as well as cloud storage services, to relay commands and extract data from compromised networks. The group relays commands via images containing hidden and encrypted data. Information is extracted from a compromised network and files are uploaded to cloud storage services.

- ## APT35

Also known as: Phosphoros and Newscaster Team

Suspected attribution: Middle East, these hackers are dynamic, often using creativity, deception, and social engineering to trick users into compromising their own computers

Sponsor: State-sponsored

Target sectors: U.S. Western Europe, and Middle Eastern military, diplomatic, and government personnel, organizations in the media, energy, and defense Industrial base, and engineering, business services, and telecommunications sectors

Motivation: Information theft and espionage

Overview: APT35 is an Iranian government-sponsored cyber espionage team that conducts long-term, resource-intensive operations to collect strategic intelligence. Mandiant Threat Intelligence has observed APT35 operations dating back to 2014. APT35 has historically relied on marginally sophisticated tools, including publicly available webshells and penetration testing tools, suggesting a relatively nascent development capability. However, the breadth and scope of APT35's operations, particularly as it relates to its complex social engineering efforts, likely indicates that the group is well resourced in other areas.

Associated malware: ASPXSHELLSV, BROKEYOLK, PUPYRAT, TUNNA, MANGOPUNCH, DRUBOT, HOUSEBLEND

Best Known Compromise: Election interference attempts (2020)

Attack vectors: APT35 typically relies on spear phishing to initially compromise an organization, often using lures related to health care, job postings, resumes, or password policies. However, also observed the group using compromised accounts with credentials harvested from prior operations, strategic web compromises, and password spray attacks against externally facing web applications as additional techniques to gain initial access.

- **APT14**

  Also known as: Anchor Panda

  Suspected attribution: Asia-Pacific: Home to large, bureaucratic hacker groups who pursue many goals and targets in high-frequency, brute-force attacks.

  Sponsor: State-sponsored, People's Liberation Army (PLA) Navy

  Target sectors: Government, telecommunications, and construction and engineering.

  Motivation: Information theft and espionage

  Overview: APT14 engages in cyber operations where the goal is data theft, with a possible focus on military and maritime equipment, operations, and policies. The stolen data, especially encryption and satellite communication equipment specifications, could be used to enhance military operations, such as intercepting signals or otherwise interfering with military satellite communication networks.

  Associated malware: Gh0st, POISONIVY, CLUBSEAT, GROOVY

  Best Known Compromise: Steal military research secrets from US universities 2017

  Attack vectors: APT14 threat actors do not tend to use zero-day exploits, but may leverage those exploits once they have been made public. They may leverage a custom Simple Mail Transfer Protocol (SMTP) mailer tool to send spear phishing messages. APT14 phishing messages are often crafted to appear to originate from trusted organizations.

Advanced Persistent Threats Potential Targets

In general, APTs target higher-value targets like other nation-states or rival corporations. Two telling characteristics of an APT attack are an extended period, and consistent attempts at concealment.

Any sensitive data is a target for an APT. Potential targets include:

- Intellectual property (e.g., inventions, trade secrets, patents, designs, processes)
- Classified data
- Personally Identifiable Information (PII)
- Infrastructure data
- Access credentials
- Sensitive or incriminating communications

Given the nature of APTs as described in the previous sections, organizations should leverage the CSF to architect a layered cybersecurity strategy in planning protections against APTs.

NIST Cybersecurity Framework

The NIST CSF provides a set of guidelines that are easily prioritized and customizable to best suit the needs of an organization. The CSF identifies five high level functions: Identify, Protect,

Detect, Respond, and Recover. These five functions are not only applicable to cybersecurity risk management but may also serve in the planning and prevention of APTs.

The CSF can help organizations respond to and contain the impact of an APT incident if one does occur. Properly detecting, containing, and reporting an APT incident is a major aspect of the Framework. When an organization has set procedures to follow in the event of a data breach, organizations can respond quickly and reduce risks as much as possible. The illustration below depicts the five core functions of the CSF.

Despite the stealthy nature of APT attacks, there are preventative measures organizations can take to protect themselves against the loss of critical information. One of the most important steps in protecting against APTs is to have layered cybersecurity protections in place. This will not only help to prevent APTs, but will also ensure that an organization's most sensitive data would remain protected if an APT attack were to happen.

When organizations implement the CSF, there are key considerations that should be evaluated when buying products, solutions, and services from APT vendors. These key considerations are discussed in the next section.

Key Considerations for APT Products, Solutions, and Services

On some level, nearly all security vendors can claim to provide an APT offering in detecting, responding to, or preventing the spread of APTs. Combating APTs requires a combination of TTPs that ideally work in a somewhat synergistic manner.

APT protections are a set of integrated solutions for the detection, prevention, and possible remediation of APT attacks. APT solutions may include, but are not limited to, sandboxing, Endpoint detection and response (EDR), Cloud Access Security Broker (CASB), reputation networks, threat intelligence management and reporting, forensic analysis and more. Some of the leading players in this market include, but not limited to, Carbon Black, CrowdStrike, FireEye, Forcepoint, Fortinet, McAfee, Microsoft, Palo Alto Networks, Sophos, Symantec, and Webroot.

Vendors in the APT vendor space should be evaluated by organization acquisition professionals according to, but to limited to, the following key technical features and capabilities:

- **Deployment Options** – availability of the solution in different form factors, such as on-premises solutions, cloud-based services, hybrid, appliances and/or virtual appliances.
- **Platform Support** – support for threat protection across a variety of platforms including: Windows, macOS, Linux, iOS, and Android.
- **Malware detection** – usually based on behavior analysis, reputation filtering, advanced heuristics, and more.
- **Firewall & URL** – filtering for attack behavior analysis.
- **Web and Email Security** – serve to block malware that originates from Web browsing or emails with malicious intent.
- **SSL/TLS scanning** – traffic over a Secure Socket Layer (SSL)/Transport Layer Security (TLS) connection is also commonly monitored to enforce organizational policies.
- **Encrypted traffic analysis** – provides monitoring of behavior of encrypted traffic to detect potential attacks.
- **Forensics and Analysis of zero-day and advanced threats** – provide heuristics and behavior analysis to detect advanced and zero-day attacks.
- **Sandboxing and Quarantining** – offer detection and isolation of potential threats.
- **Endpoint Detection and Response (EDR)** – the ability to continuously monitor endpoints and network events to detect internal or external attacks and enable rapid

response. EDR systems feed information into a centralized database where it can be further analyzed and combined with advanced threat intelligence feeds for a full understanding of emerging threats. Some EDR systems also integrate with sandboxing technologies for real-time threat emulation. Most EDR systems integrate with forensic solutions for deeper attack analysis.

- **Directory Integration** – integration with Active Directory or Lightweight Directory Access Protocol (LDAP), to help manage and enforce user policies.
- **Cloud Access Security Broker (CASB)** – on-premises or cloud-based solutions that sit between users and cloud applications to monitor all cloud activity and enforce security policies. CASB solutions can monitor user activity, enforce security policies, and detect hazardous behavior, thus extending an organization's security policies to cloud services.
- **Data Loss Prevention (DLP)** – allows organizations to define policies to prevent loss of sensitive electronic information.
- **Mobile Device Protection** – the inclusion of Mobile Device Management (MDM) or Enterprise Mobility Management (EMM) features to help protect mobile endpoints.
- **Administration** – easy, single pane of glass management across all users and network resources.
- **Real-time updates** – to rapidly block, quarantine and defend against newly identified threats or attacks across all network resources.
- **Environment threat analysis** – to detect existing threat exposure and potential security gaps.
- **Remediation** – refers to the ability to automatically restore endpoints, servers, and other devices to a healthy state, in the event they have been compromised. Remediation may involve re-imaging and/or other cleanup processes and techniques.

In addition, the following non-technical aspects should be considered

- **Pricing** – what is the pricing model for the solution, is it easy to understand and allows customers to budget properly for the solution, as well as is it in line with the level of functionality being offered, and does it represent a "good value".
- **Customer Support** – is customer support adequate and in line with customer needs and response requirements.

- **Professional Services** – does the vendor provide the right level of professional services for planning, design, and deployment, either through internal teams, or through partners.

Fortunately, several APT protection vendors that offer products and services that keep APTs at bay are on GSA's Service Schedules. The table below provides a list of GSA Service Schedules that can assist an organization in developing a holistic APT solution.

The Cybersecurity and Infrastructure Security Agency (CISA), Office of the Director of National Intelligence (ODNI), National Security Agency (NSA) and others have emphasized that APTs are conducted by highly sophisticated actors, who are patient, and by the very nature of APT, persistence is their key goal. What this means is defenders require very high skill levels with knowledge and experience in detecting and eradicating APT actors from Federal government systems.

In addition, GSA can assist in providing language for solicitations to select companies with a proven track record with eradicating APT. GSA can also provide scope reviews of the language before the solicitation goes out.

Contact information for this APT Buyer's Guide

Contact information for this APT Buyer's Guide:

- ITSecurityCM@gsa.gov for Customer Support with the APT Buyer's Guide
- RMASS@gsa.gov for any APT buyer's guide comments, suggestions, options
- Reach out to respective acquisition support for the contracts identified in the Appendix A and Appendix B of this APT Buyer's Guide

Appendix A - GSA Products and Services

A.1 GSA Product Schedules and BPAs

The below table lists GSA Product Schedules and Blanket Purchase Agreements (BPAs).

GSA Product Schedules and BPAs		
Category	**Link**	**Description**
Continuous Diagnostics and Mitigation (CDM)	GSA ADVANTAGE CDM APL TOOLS	Continuous Diagnostics and Mitigation (CDM) Tools includes Department of Homeland Security (DHS) Approved Products List (APL) hardware and software. CDM capabilities include: Asset Management, Identity and Access Management, Network Security Management, and Data Protection Management.
Alliant 2	GSA eLIBRARY ALLIANT 2	IT Security and Cybersecurity: Development and implementation of management, operational, and technical security controls required by agencies to assure desired levels of protection for IT systems and data are achieved. System and Network Controls: Facilitate the planning, organizing, coordinating, and controlling of the arrangement of the elements of protection and monitoring capabilities, and incident recovery actions of the information environment.
Miscellaneous - Complementary Special Item Numbers (SINs)	GSA eLIBRARY MISC SINS	Order-Level Materials (OLM) - are supplies and/or services acquired in direct support of an individual task or delivery order placed against a Schedule contract or BPA.
GSA Advantage	GSA ADVANTAGE	SolarWinds top alternatives in IT Infrastructure Monitoring Tools for GSA agency customers that can be purchased on GSA Advantage are provided in the links below: https://www.gartner.com/reviews/market/it-infrastructure-monitoring-tools/vendor/solarwinds/alternatives https://www.gartner.com/reviews/market/it-infrastructure-monitoring-tools

A.2 GSA Service Schedules and BPAs

The below table lists GSA Service Schedules and Blanket Purchase Agreements (BPAs).

GSA Services Schedules and BPAs		
Category	**Link**	**Description**
Highly Adaptive Cybersecurity Services (HACS)	GSA eLIBRARY 54151	Highly Adaptive Cybersecurity Services (HACS) Includes a wide range of fields such as, the seven-step Risk Management Framework services, information assurance, virus detection, network management, situational awareness and incident response, secure web hosting, and backup, security services, and Security Operations Center (SOC) services. HACS subcategories include High Value Asset Assessments, Risk and Vulnerability Assessments, Cyber Hunt, Incident Response, and Penetration Testing.
IT Professional Services	GSA eLIBRARY 5451S	IT Professional Services and/or labor categories for database planning and design; systems analysis, integration, and design; programming, conversion, and implementation support; network services, data/records management, and testing.
Identity, Credentialing, and Access Management (ICAM)	GSA eLIBRARY 541519ICAM	Identity, Credentialing and Access Management (ICAM) Managed service offerings for electronic credentials, identity and access management, authentication, and identity and access management professional services.
Data Breach Response and Identity Protection Services (IPS)	GSA eLIBRARY 541990IPS	Data Breach Response and Identity Protection Services include but are not limited to: breach mitigation and analysis/forensic services, the deployment of financial risk assessment and mitigation strategies and techniques; improvement of capabilities through the reduction, identification, and mitigation of risks; detailed risk statements, risk explanations, and mitigation recommendations; design and development of new business applications, processes, and procedures in response to risk assessments; and ensuring compliance with governance and regulatory requirements. This Scope also provides for Data Breach Response and Identity Protection Services (IPS) which includes an integrated, total solution for services to provide identity monitoring and notification of Personally Identifiable Information (PII) and Protected Health Information

		(PHI), identity theft insurance and identity restoration services, and protect (safeguard) the confidentiality of PII and PHI. Additional requirements specifically for Identity Protection Services are found in the NAICs document 541990 titled Risk Assessment, Mitigation Services, and Identity Protection.
Risk Assessment and Mitigation Services	GSA eLIBRARY 541990RISK	Risk Assessment and Mitigation Services includes: breach mitigation and analysis/forensic services, the deployment of financial risk assessment and mitigation strategies and techniques; improvement of capabilities through the reduction, identification, and mitigation of risks; detailed risk statements, risk explanations and mitigation recommendations; design and development of new business applications, processes, and procedures in response to risk assessments; and ensuring compliance with governance and regulatory requirements. Firms can assist the Ordering Agency with preventive measures in protecting Personally Identifiable Information (PII) and Protected Health Information (PHI) through the evaluation of threats and vulnerabilities to PII and PHI type of information; training of Government personnel on how to prevent data breaches and identity theft; vulnerability assessments; privacy impact and policy assessments; review and creation of privacy and safeguarding policies; prioritization of threats; maintenance and demonstration of compliance; and evaluation and analysis of internal controls critical to the detection and elimination of weaknesses to the protection of PII and PHI type of information.
Miscellaneous - Complementary Special Item Numbers (SINs)	GSA eLIBRARY MISC SINS	Order-Level Materials (OLM) are supplies and/or services acquired in direct support of an individual task or delivery order placed against a Schedule contract or BPA.
8ASTARS 2	GSA eLIBRARY 8STARS 2	8(a) Streamlined Technology Acquisition Resources for Services (STARS II) GWAC is designed to promote small business utilization when purchasing information technology (IT) services or IT services-based solutions for the federal government. Each of the 8(a) STARS II constellations includes four functional areas designated by the North American Industry Classification System (NAICS). These NAICS functional areas are:

		▪ 541511 Custom Computer Programming Services ▪ 541512 Computer Systems Design Services ▪ 541513 Computer Facilities Management Services ▪ 541519 Other Computer Related Services
Alliant 2	GSA eLIBRARY ALLIANT 2	The Alliant 2 GWAC is a multiple-award, indefinite-delivery, indefinite-quantity GWAC that will enable federal civilian agencies and the DOD to provide Information Technology (IT) services and IT services-based solutions. The basic contract offers IT solutions worldwide including Infrastructure and related services, Applications and related services, and IT Management Services to support agencies' integrated IT solution requirements. IT Security and Cybersecurity: Development and implementation of management, operational, and technical security controls required by agencies to assure desired levels of protection for IT systems and data are achieved. System and Network Controls: Facilitate the planning, organizing, coordinating, and controlling of the arrangement of the elements of protection and monitoring capabilities, and incident recovery actions of the information environment.
VETS 2	GSA eLIBRARY VETS 2	Veterans Technology Services 2 (VETS 2) is a multiple award, indefinite-delivery, indefinite-quantity GWAC set aside exclusively for service-disabled veteran-owned small business firms. VETS 2 provides Federal agencies with customized IT services and IT services-based solutions, both commercial and non-commercial.

Appendix B - Continuous Diagnostics and Mitigation (CDM) Program: Dynamic and Evolving Federal Enterprise Network Defense (DEFEND A-F)

These orders were placed against the Alliant 2 Government wide Acquisition Contracts (GWAC) with the goal of defending Federal IT networks from cyber security threats. This is an Assisted Acquisition Solution that includes the end-to-end acquisition for all Civilian Agencies.

B.1 Products and services available on the DEFEND orders

- Continuous monitoring sensors (tools), diagnosis, mitigation tools, and associated services to strengthen the security posture of Government networks. The tools that CDM has implemented for the Agencies include BigFix (HCL), Forescout, Cisco ISE, Tenable, Splunk, RSA Archer, and Elastic. Ability to add other emerging technologies.
- Services include surge support to aid Agencies impacted by cyber-attacks, in need of penetration testing, or requiring cyber risk assessment and mitigation activities. Activities may include incident response, threat hunting, forensic analysis, and remediation activities. CDM can also deploy, configure, and integrate Agency requested cyber tools and services.

B.2 Products and services available to specifically assist with SolarWinds issue:

- Asset management sensor tools to detect the presence of SolarWinds
- Identity and access management tools to mitigate unauthorized access
- Services to re-architect networks, deploy additional tools, and implement new governance processes as part of SolarWinds remediation efforts

B.3 How to get assistance:

Agencies should contact the CISA Technical Point of Contact (POC) to establish a request for service. This is then processed and sent to GSA along with funding. GSA will manage the procurement process and contract administration in partnership with CISA.

DEFEND POCs	
Defend	**Agencies**
DEFEND A DHS: markita.poindexter@cisa.dhs.gov GSA: r8.defend.a@gsa.gov	a. Department of Homeland Security b. CISA Headquarters c. United States Coast Guard d. Federal Emergency Management Agency e. DHS Federal Law Enforcement Training Center f. Customs and Border Protection g. DHS/CISA/CSD/FNR

DEFEND B DHS: colleen.mcdarby@cisa.dhs.gov GSA: r8.defend.b@gsa.gov	a. Executive Office of the President (EOP) of the United States (Office of Management and Budget (OMB) MAX) b. United States Department of Energy (DOE) c. United States Department of Interior (DOI) d. United States Department of Transportation (DOT) e. United States Office of Personnel Management (OPM) f. United States Department of Agriculture (USDA) g. United States Department of Veteran Affairs (VA)
DEFEND C DHS: joseph.sheridan@hq.dhs.gov GSA: r8.defend.c@gsa.gov	a. Department of Homeland Security b. Department of State c. Department of Labor d. Department of Commerce e. Agency for International Development
DEFEND D DHS: colleen.mcdarby@cisa.dhs.gov GSA: r8.defend.d@gsa.gov	a. The United States General Services Administration (GSA) b. The United States Department of Health and Human Services (HHS) c. The United States National Aeronautics and Space Administration (NASA) d. The United States Social Security Administration (SSA) e. The United States Department of Treasury (Treasury) f. The United States Postal Service (USPS)
DEFEND E DHS: rita.wilson@hq.dhs.gov GSA: r8.defend.e@gsa.gov	a. Department of Homeland Security b. National Science Foundation c. Federal Deposit Insurance Agency d. US Department of Education e. DHUD-ASST SEC FOR ADMIN-IMMED OFC f. Small Business Administration (SBA) g. US Nuclear Regulatory Commission
DEFEND F DHS: jason.neumer@cisa.dhs.gov GSA: r8.defend.f@gsa.gov	a. Department of Homeland Security