C3 VOLUNTARY PROGRAM

Cybersecurity Service Offering Reference Aids

Safeguarding the cybersecurity of America's infrastructure is critical to our Nation's economic viability and global competitiveness. It is a national priority that is shared among a host of public departments and agencies and private sector entities.

The nature of business and commercial operations has evolved in many ways. Our Nation's dynamic commercial landscape requires a substantial depth and breadth of cybersecurity knowledge and expertise just to comprehend threats to and the diversity of consequences that may potentially impact organizations. The Nation is rapidly transitioning to Internet Protocol based communications with new service offerings emerging daily. The "Internet of Things", a term used to describe the interconnected environment of "E-Enabled" devices (devices that are connected to the Internet), is a rapidly evolving environment. Cloud computing capabilities are being used as the backbone for critical services because of their relatively inexpensive distribution mechanisms. These offerings are ushering in an array of challenges to the overall security and resilience of our National infrastructure and heightening the need for solutions to those challenges.

In many cases, the capability and complexity of the range of services necessary to defend against cyber threats far exceeds the potential for improved security and resilience that organizations can achieve in-house. To remain operationally viable as well as commercially competitive, many entities are looking to external service providers to identify, assess solutions for, and deliver scalable and affordable security services to achieve a desired level of resilience. Purchasing cybersecurity services may often be the greatest incremental contribution to effective cybersecurity and resilience that an organization can make. However, in order to get the most benefit from cybersecurity services, entities should take careful notice of the terms of their contracts and service level agreements to ensure that their needs are adequately met.

The Department of Homeland Security's National Protection and Programs Directorate leads the Federal Government's public-private cybersecurity coordination. In executing that role, the Department works with public as well as private sector entities and is in a position to identify best practices, lessons-learned, and specific controls to meet emerging challenges.

The list below includes freely-available reports and resources pertinent to managing the acquisition of cybersecurity services. It is not intended to be exhaustive, but covers a wide range of cybersecurity services including cloud service providers, cyber incident response, cloud computing, software assurance, and industrial control systems. While most of the recommendations and reports below are vendor-agnostic, some identify specific service providers that have met a certification criteria related to their service offerings.

DHS does not endorse any particular service provider or offering. DHS also expressly does not warrant the adoption of any practice, course of action, or the incorporation of any recommended language to be advantageous in a particular situation or circumstance. The information below is provided as-is and solely for thoughtful consideration within the appropriate due diligent decision-making and planning deemed necessary to identify and evaluate cybersecurity service provider offerings.

Department of Homeland Security

Cybersecurity Procurement Language for Control Systems

(http://ics-cert.us-cert.gov/sites/default/files/documents/Procurement_Language_Rev4_100809.pdf)

Based on a joint effort of public and private sector entities, this document illustrates common procurement language for use by all industrial control system stakeholders. The contract language in this document is intended to be sector-agnostic and provide common control system procurement guidelines that can be incorporated into contracts regardless of the entities involved.

- **Focus Area:** Industrial Control Systems
- **Includes contract language examples:** Yes
- **Includes specific vendor list:** No

Software Assurance in Acquisition and Contract Language

(https://buildsecurityin.us-cert.gov/sites/default/files/AcquisitionAndContractLanguage_PocketGuideV1%202_05182012_PostOnline.pdf)

A resource for selecting and adopting relevant practices for delivering secure software, this guide identifies sample contract language for integrating software security into the acquisition life cycle.

- **Focus Area:** Software
- **Includes contract language examples:** Yes
- **Includes specific vendor list:** No

Software Supply Chain Risk Management and Due Diligence

(https://buildsecurityin.us-cert.gov/sites/default/files/DueDiligenceMWV12_01AM090909.pdf)

This guide provides a list of relevant questions and issues to consider when procuring software from a variety of sources. The guide differs from the Software Assurance guide in that it does not include specific contract language, but rather provides a series of questionnaires that can be used to guide acquisition decision-making with an emphasis on supply chain risk management.

- **Focus Area:** Software
- **Includes contract language examples:** No
- **Includes specific vendor list:** No

Department of Defense

DoD Enterprise Cloud Service Broker: Cloud Security Model

(*http://iase.disa.mil/cloud_security/index.html*)

This document establishes DoD security requirements for cloud service providers to host DoD mission assets up to and including SECRET information. The various appendices highlight a number of specific controls and precise language for use in government contracts.

- **Focus Area**: Cloud Service Providers
- **Includes contract language examples:** Yes; Appendix M provides a list of DoD-specific security controls for consideration/inclusion in service level agreements/contracts.
- **Includes specific vendor list**: No

Department of Energy

Cybersecurity Procurement Language for Energy Delivery System Energy Sector Control Systems Working Group

(*http://energy.gov/sites/prod/files/2014/04/f15/CybersecProcurementLanguage-EnergyDeliverySystems_040714_fin.pdf*)

Stems from DOE and DHS collaboration with industry subject matter experts in 2009 for the *Cyber Security Procurement Language for Control Systems*, designed to give general recommendations, principles, and controls to consider when procuring control systems products and services. This guide is an updated version of that original document.

- **Focus Area:** Energy Delivery Systems
- **Includes contract language examples**: Yes
- **Includes specific vendor list**: No

General Services Department / Department of Homeland Security

Continuous Diagnostics and Mitigation Program: Tools and Continuous Monitoring as a Service (Blanket Purchase Agreements)

(*http://www.gsa.gov/portal/mediaId/189495/fileName/CMaaS_Ordering_Guide_V40_Mar2014_v2.action*)

This document outlines the ordering options for services being offered through GSA Blanket Purchase Agreements as well as a list of companies that have been awarded Blanket Purchase Agreements for Continuous Diagnostics and Mitigation. The scope of the Blanket Purchase Agreements will ultimately include 15 Tool Functional Areas and 11 Continuous Monitoring-as-a-Service task areas, however at the time of this writing only 4 Tool Functional Areas are available.

- **Focus Area:** Continuous Diagnostics and Mitigation
- **Includes contract language examples**: No
- **Includes specific vendor list**: Yes

Risk Management Framework Services (Blanket Purchase Agreements)

(*http://www.gsa.gov/portal/getMediaData?mediaId=154783*)

This document outlines the ordering options for services being offered through GSA Blanket Purchase Agreements for Risk Management Framework cyber security services (formerly known as Certification & Accreditation).

- **Focus Area**: Risk Management Framework
- **Includes contract language examples:** No
- **Includes specific vendor list**: Yes

National Security Agency

National Security Cyber Assistance Program

(*http://www.nsa.gov/ia/programs/cyber_assistance_program/*)

This program creates an accreditation framework for evaluation commercial cyber-assistance service providers against industry best practices and NSA-developed criteria. The program is currently looking at Cyber Incident Response Assistance as the first accreditation in the series, using a series of 21 focus areas.

- **Focus Area:** Cyber Incident Response (currently)
- **Includes contract language examples:** No
- **Includes specific vendor list:** Yes

National Institute of Science and Technology

Special Publication 800-146: Cloud Computing Synopsis and Recommendations

(*http://csrc.nist.gov/publications/nistpubs/800-146/sp800-146.pdf*)

This document provides NIST guidance and recommendations on a variety of cloud computing environments, including Software-as-a-Service, Platform-as-a-Service, Infrastructure-as-a-Service, and general cloud computing. The document includes a description of common contractual terms of service, practical security considerations for each of the different environments, and recommendations for best practices.

- **Focus Area:** Cloud Computing
- **Includes contract language examples**: No, but does describe common terms of service
- **Includes specific vendor list**: No

Other

Cloud Security Alliance

Critical Areas of Focus in Cloud Computing V3.0

(https://downloads.cloudsecurityalliance.org/initiatives/guidance/csaguide.v3.0.pdf)

This document provides a set of best security practices for 14 domains involved in governing or operating cloud services including Software-as-a-Service, Platform-as-a-Service, and Infrastructure-as-a-Service.

- **Focus Area**: Cloud Service Providers
- **Includes contract language examples**: No, but does include issues for consideration
- **Includes specific vendor list**: No

United Kingdom Centre for the Protection of National Infrastructure

Cyber Incident Response Service

(http://www.cpni.gov.uk/advice/cyber/cir/)

This program, operated by the UK Centre for Protection of National Infrastructure, certifies select industry partners which deliver cyber incident response services that are focused on responding to sophisticated targeted attacks against networks of national significance. The service providers must submit applications and are subsequently selected and listed on the website.

- **Focus Area:** Cyber Incident Response
- **Includes contract language examples**: No
- **Includes specific vendor list**: Yes