



November
2019

THE ICIT FEDERAL AGENCY INITIATIVE REPORT

A MONTHLY ANALYST REPORT FROM
THE INSTITUTE FOR CRITICAL
INFRASTRUCTURE TECHNOLOGY

ICIT | Institute for Critical
Infrastructure Technology
The Cybersecurity Think Tank

The ICIT Cyber Federal Cybersecurity Initiative Report

November 2019

A Monthly Non-Partisan Analyst Report from The Institute for Critical
Infrastructure Technology

www.icitech.org

This ICIT Analyst Report has been made publicly available. ICIT Analyst Reports are licensed to ICIT Individual and Corporate Members only.

To receive this and other ICIT Analyst Reports in the future, join ICIT at:
www.icitech.org/support-icit/

Copyright 2019 Institute for Critical Infrastructure Technology. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher. For permission requests, contact the Institute for Critical Infrastructure Technology.

Contents

About this Report	6
Census Bureau	7
Commerce IG Auditing Census Bureau's Cybersecurity Ahead of 2020 Count	7
Census Bureau Plans to Combat Misinformation with Fusion Center.....	7
Department of Defense (DOD).....	8
DoD Revises CMMC Program; Issues Version 0.6	8
DoD Finishes Second Audit; Finds 1300 Security Findings.....	8
Defense Innovation Board Releases Ethical Principles for AI	9
DoD Seeking Solution Briefs on Alternate Cloud Security Gateway.....	10
GAO Issues Report on Space Command and Control	10
DOD Publishes Final Rule Implementing Restrictions on LPTA Source Selection Process.....	11
DOD is Seeking Nonprofits for Cyber Accreditation Program.....	11
DOD Received Over 2,000 Comments on CMMC Version 0.4	11
Fresh draft of DOD contractor cybersecurity standards coming next month	12
DOD Releases Public Draft of Cybersecurity Maturity Model Certification and Seeks Industry Input...	12
DOD Streamlines Cloud Authorizations	13
DOD Inspector General Finds that Defense Contractors are Inadequately Securing Sensitive Information	13
US Navy Hosting AI Challenge.....	13
DOD Upgrading IT Infrastructure in Preparation of MHS GENESIS Implementation.....	14
9,000 Vulnerable Devices Acquired by DOD in 2018.....	14
DOD, GSA, NASA draft rules banning purchases of IT products from China	15
DOD Beginning to Prioritize 5G Investments.....	15
DOD Announces the Cybersecurity Maturity Model Certification (CMMC)	15
Navy Reimagining CIO Position.....	16
Defense Information Systems Agency.....	17
DISA starts consolidation of Fourth Estate IT	17
DISA Seeks AI-Based Solution to Cyberattacks	17
DISA Outlines Upcoming Acquisition Opportunities.....	17

DISA Seeking Vendors to Build the Unified Situational Cyber Awareness (USCA) Platform.....	19
DISA, HHS Brainstorming Behavioral-Based Identity Pilot.....	19
DISA, Cyber Command Are Launching a Zero-Trust Pilot Program	20
Department of Energy (DOE)	21
DOE Announces \$80 Million for New Grid Modernization Lab Call Projects	21
DOE Announced Three Projects to Advance Energy Sector Cybersecurity	21
DOE and NSF Partner to Launch the National AI Research Institutes Program.....	22
Department of Energy Department Launches \$5.5M AI Collaboration	22
DOE Announced Public-Private Partnerships to Accelerate AI Development	23
DOE Establishing Office for Artificial Intelligence and Technology.....	23
DOE Seeking Comment on Revised Cybersecurity Capability Maturity Model (C2M2)	24
DOE Seeking Input on Draft of Latest Cybersecurity Risk Assessment Model	24
Federal Communications Commission	26
FCC bans Chinese telecoms Huawei and ZTE from access to federal broadband subsidies.....	26
Federal Election Commission	27
OIG Finds that FEC Lacks Adequate Information Security Procedures	27
Government Accountability Office (GAO)	28
GAO Identified Cybersecurity Risks to the Electric Grid	28
Department of Homeland Security (DHS).....	29
CISA Announces Cyber Essentials for Small Business	29
CISA invests in election auditing tool to secure 2020 elections	29
DHS Seeking Feedback on Vulnerability Disclosure Program	30
CISA Indicates Plans to Fortify U.S. Election Infrastructure.....	30
DHS Establishing Transatlantic Aviation Industry Roundtable Committee to Bolster Aviation Cybersecurity	31
DHS Updating Automated Indicator Sharing Program	31
DHS Plans Fall Launch of New Continuous Diagnostics and Mitigation Dashboard.....	31
DHS Considering Changes to Staff Management for Security Operations Centers.....	32
Department of Justice (DOJ).....	33
The FBI and DOJ Opened \$100m Idaho Data Centre Hub	33
DOJ Launches the Transnational Elder Fraud Task Force	33
General Services Administration (GSA)	34

GSA and DLA Streamlining the Federal Supply Chain	34
GSA and Air Force Preparing for 5G Rollout	34
Department of Health and Human Services (HHS)	35
HHS, DISA Aim to Protect Healthcare Data with Assured Identity Pilot	35
HHS to Develop Cybersecurity Development Approaches	35
HHS Issued Proposed Rule to Update Anti-Kickback Statute Safe Harbors	35
National Institute of Standards and Technology (NIST)	37
GSA and NIST Working to Automate FedRAMP Assessments	37
NIST Partners with Microsoft on Enterprise Patch Management Guidance	37
NIST Seeking Vendor Insight on Mitigating Risk to Telehealth Cybersecurity	38
NIST Seeking Comments on Improving Health Information Protections	38
NIST Soliciting Public Input on Personal Privacy Protections	39
NIST Seeking Comment on IoT Cybersecurity Baseline	39
NIST Delays Cyber Standards for Pentagon Contractors	40
NIST Developing AI Standards	40
National Security Agency (NSA)	42
NSA Publishes Advisory Addressing Encrypted Traffic Inspection Risks	42
NSA's Cyber Directorate to Focus on Industrial Base	42
NSA Reorganizing in Anticipation of the Launch of the New Cybersecurity Directorate	42
NSA Creates New Cybersecurity Directorate	43
Office of Management and Budget (OMB)	44
OMB to name agency to lead federal IT supply chain information sharing effort	44
OMB Updates FISMA Guidance for FY2020	44
OMB Opens TIC Policy, Allows Agencies Wider Use of Cloud Services	45
Office of Personnel Management (OPM)	46
OPM Launching Rotational Program for Cyber Reskilling Academy Graduates	46
Pentagon	47
Pentagon Developing JEDI Cloud Deployment Security Guidance	47
Pentagon 'Hack the Proxy' Programme Uncovered 31 Vulnerabilities	47
US Air Force Modernizes Nuclear Weapons Management System	47
Joint AI Center Soliciting Broad Cybersecurity Pitches	47
Department of Veterans Affairs	49

GAO Finds VA Still Needs to Address Cybersecurity Issues	49
White House.....	50
White House Establishes National Quantum Initiative Advisory Committee	50

About this Report

As a non-partisan cybersecurity think tank, one of ICIT's goals is to increase access and visibility on federal agency cybersecurity and privacy related initiatives or agency decisions. This monthly members-only report is an objective summary of various federal agency programs, announcements, reports, and other initiatives deemed significant by ICIT analysts.

Readers should note the following:

- Highlighted items new initiatives added since the previous months report
 - ICIT will keep legislation on the report for 3 months
 - This report primarily tracks initiatives that ICIT analysts define as 'cyber-centric', meaning its primary focus is cybersecurity, information security or digital privacy
-

Census Bureau

Commerce IG Auditing Census Bureau's Cybersecurity Ahead of 2020 Count Introduced – October 2019

Summary

A few months out from the start of the Census Bureau's 2020 count, the Commerce Department's inspector general is running an audit of the bureau's cybersecurity measures. The IG office will work alongside the U.S. Digital Service to review the bureau's prep work for the first decennial count where the public can respond online, or over the phone. The bureau has partnered with the Department of Homeland Security, and the intelligence community, to mitigate cyber threats and misinformation.

Reference Links

- [Commerce IG auditing Census Bureau's cybersecurity ahead of 2020 count](#)
 - [Audit of the U.S. Census Bureau's IT Security Measures Supporting the 2020 Census](#)
 - [Commerce watchdog will monitor efforts to keep 2020 census secure](#)
-

Census Bureau Plans to Combat Misinformation with Fusion Center Introduced – September 2019

Summary

The Census Bureau has stood up a "fusion center" to monitor social media for misinformation during the 2020 count and has doubled down on its resilience planning in the final months of preparation. Additionally, the bureau has been working with Department of Homeland Security and members of the intelligence community on cybersecurity efforts that include red team penetration testing and monitoring social media platforms for signs of an imminent cyber threat.

Reference Links

- [Census Bureau stands up 'fusion center' to combat misinformation during 2020 count](#)
 - [Security concerns abound for internet first Census](#)
-

Department of Defense (DOD)

DoD Revises CMMC Program; Issues Version 0.6

Introduced – November 2019

Summary

In response to more than 2000 comments, on November 7, 2019, the DoD issued version 0.6 of the Cybersecurity Maturity Model Certification (“CMMC”). That new version of the draft CMMC covers 17 domains (Access Control, Asset Management, Audit and Accountability, Awareness and Training, Configuration Management, Identification and Authentication, Incident Response, Maintenance, Media Protection, Personnel Security, Physical Protection, recovery, Risk Management, Security Assessment, Situational Awareness, System and Communications Protections System and Information Integrity) and addresses the processes and practices required for levels 1 through 3. DoD advises that it is still working through the comments relating to the higher level certification processes and practices for levels 4 and 5 and that it will issue a follow-on draft addressing those additional levels in the near future.

Reference Links

- [DoD Issues Revised Draft Cyber Security Model Certification to Address Levels 1 Through 3](#)
 - [DOD Issues “Draft Version 0.6” of Its Cybersecurity Maturity Model Certification, Part of an Initiative That Likely Will Have Critical Ramifications for All Companies Seeking to Conduct Business with DOD](#)
-

DoD Finishes Second Audit; Finds 1300 Security Findings

Introduced – November 2019

Summary

The report boasts progress in completing assessments for 14 Fourth Estate agencies and 800 of their applications for data migration and center closures, and in moving networks to a single service provider. The result: DOD migrated 244 systems to enterprise-level hosting environments and closed 17 Fourth Estate data centers. The report found that 556 of 2,410 separate findings from the 2018 audit had been resolved; however, more than 1,300 new findings were discovered in the course of the second audit, in addition to the 1800 remaining issues from the 2018 audit.

Reference Links

- [DOD finishes second audit](#)
 - [DoD's second financial audit uncovers 1,300 new deficiencies](#)
-

Defense Innovation Board Releases Ethical Principles for AI

Introduced – November 2019

Summary

The Defense Innovation Board has offered guidance for how the Pentagon should use and govern artificial intelligence systems. The document lays out five key principles for the department's use of AI. AI should be:

1. Responsible: "Human beings should exercise appropriate levels of judgment and remain responsible for the development, deployment, use, and outcomes" of DOD AI systems, the document says.
2. Equitable: The Pentagon "should take deliberate steps to avoid unintended bias in the development and deployment of combat or non-combat AI systems that would inadvertently cause harm to persons."
3. Traceable: DOD's AI engineering discipline "should be sufficiently advanced such that technical experts possess an appropriate understanding of the technology, development processes, and operational methods of its AI systems, including transparent and auditable methodologies, data sources, and design procedure and documentation."
4. Reliable: DOD AI systems "should have an explicit, well-defined domain of use, and the safety, security, and robustness of such systems should be tested and assured across their entire life cycle within that domain of use," the document says.
5. Governable: Finally, the Pentagon's AI tools "should be designed and engineered to fulfill their intended function while possessing the ability to detect and avoid unintended harm or disruption, and for human or automated disengagement or deactivation of deployed systems that demonstrate unintended escalatory or other behavior."

The document also recommends enhanced training for DOD employees and service members who will be working with AI; refining reliability benchmarks as well as testing and evaluation techniques for AI; developing risk management methods for the use of AI; and the formal adoption of the board's ethics principles as DOD policy.

Reference Links

- [AI Principles: Recommendations on the Ethical Use of Artificial Intelligence by the Department of Defense](#)

- [DOD Board Lays Out Ethical Principles for AI](#)
-

DoD Seeking Solution Briefs on Alternate Cloud Security Gateway

Introduced – November 2019

Summary

The Department of Defense's (DoD) Defense Innovation Unit is currently seeking solution briefs on methods to increase operational efficiency by utilizing cloud-based systems delivered through Cloud Service Providers (CSPs) through an alternate cloud security gateway.

Reference Links

- [Defense Innovation Unit: Submit a Solution Brief](#)
 - [DoD Seeks Alternate Cloud Security Gateway](#)
-

GAO Issues Report on Space Command and Control

Introduced – November 2019

Summary

The GAO found that given emerging and evolving threats in the space domain, as well as significant development problems in similar prior efforts, the Air Force is prioritizing the Space Command and Control (C2) program.

Early prototype work on the program's software began in 2016. As of mid-2019, the program had delivered some initial capabilities; however, the capabilities delivered so far are not approved for use in operations. Because the program is still early in development, it has not yet established a time frame for certifying these capabilities for operational use. Further, the foundational elements of the program, including the infrastructure and software platform, are still being conceptualized. All Space C2 program capabilities will be significantly more automated than past development efforts and are being designed to allow operators to identify and monitor threats to U.S. space assets, identify courses of action to mitigate or eliminate those threats, communicate these actions to decision makers, and direct actions in response.

Reference Links

- [SPACE COMMAND AND CONTROL Comprehensive Planning and Oversight Could Help DOD Acquire Critical Capabilities and Address Challenges](#)

- [GAO: Space Command And Control: Comprehensive Planning and Oversight Could Help DOD Acquire Critical Capabilities and Address Challenges](#)
 - [GAO Report on Space Command and Control](#)
-

DOD Publishes Final Rule Implementing Restrictions on LPTA Source Selection Process **Introduced** – October 2019

Summary

The DOD issued a final rule to implement statutory restrictions on the use of the lowest price technically acceptable (LPTA) source selection process. The final rule is intended to address the perceived overuse of the LPTA process by establishing clear conditions that must be met before DOD agencies may utilize the LPTA process for a given source selection. The rule became effective on October 1, 2019.

Reference Links

- [Defense Federal Acquisition Regulation Supplement: Restrictions on Use of Lowest Price Technically Acceptable Source Selection Process \(DFARS Case 2018-D010\)](#)
 - [Department of Defense \(DOD\) publishes final rule implementing restrictions on the use of lowest price technically acceptable \(LPTA\) source selection process](#)
-

DOD is Seeking Nonprofits for Cyber Accreditation Program **Introduced** – October 2019

Summary

The Department of Defense is reportedly soliciting the input of nonprofits on an accreditation body for its upcoming program to rate contractors' cybersecurity. In particular, the DOD wants to know how it should establish and maintain an accreditation body for its Cybersecurity Maturity Model Certification (CMMC) program.

Reference Links

- [DOD Seeks Nonprofits For Cyber Accreditation Program](#)
-

DOD Received Over 2,000 Comments on CMMC Version 0.4 **Introduced** – October 2019

Summary

The Department of Defense is making progress on both its Cybersecurity Maturity Model Certification (CMMC) and a new policy on software development in the department. The model, being developed in partnership with experts at Johns Hopkins and Carnegie Mellon, establishes five levels of maturity across 18 domains and many capabilities. The certification accreditation will be run by a nonprofit organization – a request for information is out for that organization. A fresh draft of the CMMC is expected to debut in November 2019. The final CMMC version 1.0 will go to the CMMC accreditation body in January 2020. The first requests for information that include CMMC requirements are set for release in June 2020 and the corresponding requests for proposals are slated for that fall.

Reference Links

- [DOD Offers Updates on Acquisition Reforms](#)

Fresh draft of DOD contractor cybersecurity standards coming next month

DOD Releases Public Draft of Cybersecurity Maturity Model Certification and Seeks Industry Input

Introduced – September 2019

Summary

The Office of the Assistant Secretary of Defense for Acquisition has released Version 0.4 of its draft Cybersecurity Maturity Model Certification (CMMC) for public comment. The DoD describes the draft CMMC framework as a “unified cybersecurity standard” for DoD acquisitions that is intended to build upon existing regulations, policy, and memoranda by adding a verification component to cybersecurity protections for safeguarding Controlled Unclassified Information (CUI) within the DIB. The DoD has stated that it intends to release Version 1.0 of the CMMC framework in January 2020 and will begin using that version in new DoD solicitations starting in Fall 2020. Notwithstanding the pendency of these deadlines, a large number of questions remain outstanding. The DoD is seeking feedback on the current version of the model by September 25, 2019.

Reference Links

- [DoD Releases Public Draft of Cybersecurity Maturity Model Certification and Seeks Industry Input](#)
 - [Pentagon Issues Draft Cybersecurity Certification Framework](#)
 - [DoD unveils new cybersecurity certification model for contractors](#)
 - [DOD Will Require Vendor Cybersecurity Certifications By This Time Next Year](#)
-

DOD Streamlines Cloud Authorizations

Introduced – August 2019

Summary

The Defense Information Systems Agency, within DoD, issued a blanket provisional authorization to streamline cloud authorizations department-wide. Cloud service providers no longer need the Department of Defense's go-ahead to store unclassified information in Federal Risk and Authorization Management Program-approved, moderate baseline offerings.

Reference Links

- [It's Official: Defense Department Will Use Other Agencies' Cloud Security Assessments](#)
 - [DOD streamlines cloud authorizations, as promised](#)
-

DOD Inspector General Finds that Defense Contractors are Inadequately Securing Sensitive Information

Introduced – August 2019

Summary

The DOD inspector general released a report July 25 after reviewing how DOD information is protected on contractor's networks and systems. The IG found that contractors were not consistently adhering to DOD's cybersecurity standards, which are based on controls created by the National Institute of Standards and Technology. Specifically the report found that, contractors failed to use multifactor authentication, enforce strong password use, identify and mitigate vulnerabilities or document and track cybersecurity incidents. Administrators also improperly assigned access privileges that did not align with users' responsibilities.

Reference Links

- [Defense contractors aren't securing sensitive information, watchdog finds](#)
 - [DOD Contractors Leaving Gov't Info At Risk, Watchdog Says](#)
 - [Uncontrolled Information: DoD Audit Finds Contractor Lapses in Protecting Controlled Unclassified Information](#)
-

US Navy Hosting AI Challenge

Introduced – August 2019

Summary

The Naval Information Warfare Systems Command is holding an AI cybersecurity challenge in conjunction with the Program Executive Office for Command, Control, Communications, Computers and Intelligence. The goal is to automate cybersecurity operations using AI and machine learning. The challenge, which is dubbed AI Applications to Autonomous Cybersecurity or AI ATAC (pronounced attack), is offering \$150,000 to individuals, academia or businesses (First prize will receive \$100,000 and second will get \$50,000).

Reference Links

- [The Navy will pay you for AI software that detects cyber attacks](#)
-

DOD Upgrading IT Infrastructure in Preparation of MHS GENESIS Implementation Introduced – August 2019

Summary

The Department of Defense is focusing on three areas, area network infrastructure, medical device cybersecurity, and enterprise services architecture, in upgrading its healthcare IT infrastructure in preparation for implementation of its new Cerner-based MHS GENESIS electronic health record (EHR) system. MHS GENESIS will replace legacy DoD EHR systems, including the Armed Forces Health Longitudinal Technology Application, the Composite Health Care System, and components of the Theater Medical Information Program-Joint. It will support more than 9.5 million DoD beneficiaries and 205,000 military health system personnel.

Reference Links

- [DoD Tackles Healthcare IT Infrastructure Upgrades for MHS GENESIS](#)
-

9,000 Vulnerable Devices Acquired by DOD in 2018 Introduced – August 2019

Summary

According to an audit released by the Pentagon Inspector General, more than 9,000 commercially available information technology products bought by the DoD in fiscal year 2018 could be used to spy on or hack U.S. military personnel and facilities. Without fixing oversight of such purchases, more risks lie ahead, potentially including perils for top-dollar weapons that use such “commercial-off-the-shelf” or COTS devices.

Reference Links

- [DoD Bought Chinese Tech Vulnerable to Spying, Hackers](#)
 - [Official Cybersecurity Review Finds U.S. Military Buying High-Risk Chinese Tech](#)
-

DOD, GSA, NASA draft rules banning purchases of IT products from China

Introduced – August 2019

Summary

The Defense Department, General Services Administration and NASA have drafted interim final regulations for banning the government's purchases of IT and video surveillance equipment and components from Huawei and other China-based tech firms, a move that will likely fuel growing tensions between Washington and Beijing. The regulations will go into effect in mid-August and are required by the Fiscal Year 2019 National Defense Authorization Act.

Reference Links

- [DOD, GSA, NASA draft rules banning purchases of IT products from China](#)
-

DOD Beginning to Prioritize 5G Investments

Introduced – August 2019

Summary

Due to how ubiquitous 5G networks are expected to be in the near future and how important it is that the United States be part of its development, the DOD is expected to highlight significant investments into 5G infrastructure in the 2021 budget that is being submitted to the Office of Management and Budget for approval.

Reference Links

- [Top DoD scientist to start prioritizing 5G in investments](#)
-

DOD Announces the Cybersecurity Maturity Model Certification (CMMC)

Introduced – August 2019

Summary

The U.S. Department of Defense (DoD) has announced that it will be rolling out a new cybersecurity certification model for private companies who hold contracts with the DoD. The model is called the Cybersecurity Maturity Model Certification (CMMC). The development of this model is an evolution in

the DoD's effort to protect the U.S. defense supply chain from foreign and domestic cybersecurity threats.

Reference Links

- [DoD Will Require New Cybersecurity Standards in 2020: Could Other Agencies Be Next?](#)
 - [U.S. Department of Defense Announces New Cybersecurity Model for DoD Contractors](#)
-

Navy Reimagining CIO Position

Introduced – August 2019

Summary

The Navy is making major changes at its senior levels by creating a new special assistant to the secretary that will oversee cybersecurity, data and information. The special assistant will oversee four directorates:

- The Navy's chief technology office, which will be responsible for guiding acquisition and priorities around the technical infrastructure;
- The service's chief digital strategy office, which will be responsible for moving the Navy into a digital era by leveraging applications, adopting best commercial practices and managing digital information;
- The Navy's chief data office, which will help structure data that can be used in areas such as artificial intelligence and analytics;
- A chief information security/cybersecurity office that will help guide the Navy through a cultural shift to improve poor cyber hygiene, which has been the culprit for major breaches.

Reference Links

- [The Navy thinks it has a better idea for a CIO position](#)
 - [New official will oversee all IT, cyber issues for Navy, Marine Corps](#)
-

Defense Information Systems Agency

DISA starts consolidation of Fourth Estate IT

Introduced – November 2019

Summary

The Defense Information Systems Agency has begun to move its clients to DODNet, the new single service network for support defense agencies and field activities. The Fourth Estate Network Optimization program will migrate five agencies to DODNet and Defense Enclave Services in an effort to consolidate commonly used IT services, such as help desk support, by the end of fiscal 2021.

Defense Technical Information Center (DTIC), Defense Media Activity, Defense Personnel Accounting Agency (DPAA), Defense Microelectronics Activity, and DISA will be the first of a total of 14 agencies to migrate with the aim of eliminating redundancy and letting defense organizations focus on their missions rather than IT services.

Reference Links

- [DISA starts Fourth Estate IT consolidation](#)
 - [DISA Begins Transition to DoDNET IT Services Hub](#)
 - [DISA Begins Implementing Fourth Estate Initiative](#)
-

DISA Seeks AI-Based Solution to Cyberattacks

Introduced – November 2019

Summary

The Defense Information Systems Agency (DISA) released a request for information on artificial intelligence (AI) and machine learning (ML) technologies that can detect and combat cyberattacks as they occur. The agency is interested in minimizing the time to “detect, respond to, and, ultimately, mitigate attacks” via an automated solution.

Reference Links

- [DISA Seeks AI-Based Solution to Cyberattacks](#)
 - [DISA Is Looking to Buy AI-Powered Cyber Defenses](#)
-

DISA Outlines Upcoming Acquisition Opportunities

Introduced – November 2019

Summary

DISA announced upcoming FY2020 industry awards for information technology (IT) projects and initiatives. Areas of interest ranged from embracing emerging technologies to improving endpoint security, but many plans lacked a detailed acquisition strategy. Acquisition opportunities for FY 2021 and 2022 in areas such as secure configuration management, enterprise mission assurance support, and continuous monitoring and risk scoring, were also announced.

First Quarter RFPs

- **Cyber Training Development and Delivery:** An RFP to develop Cyber Training for Classroom and Online delivery will be released. DISA plans to award a single contract for the project through a small-business set aside in the second quarter.
- **Web Content Filtering (WCF):** An RFP on the engineering and sustainment of the WCF system will be released. DISA plans to award a single Encore III contract for the project after a full and open competition in the third quarter.
- **Unified Cyber Situational Awareness (UCSA):** An RFP to provide trained, experienced, and high-quality IT and cybersecurity engineering and innovation labor support will be released. DISA plans to award a single contract for the project in the third quarter.

Second Quarter RFPs

- **Endpoint Detection and Response:** An RFP for new endpoint security capabilities allowing cyber defenders to quickly detect, investigate and mitigate security incidents will be released. DISA plans to award a single contract for the project in the third quarter.
- **Application Containment:** An RFP for endpoint security capabilities providing the ability to restrict execution of high-risk applications and computer processing activities to an isolated environment will be released. DISA plans to award a single contract for the project in the third quarter.
- **SHARKSEER:** An RFP to provide web-based zero-day network defense and advanced persistent threat protection will be released. DISA plans to award a single contract for the project via a full and open competition in the third quarter.
- **Comply to Connect:** An RFP for a framework of tools and technologies that restrict unauthorized access, reduce vulnerabilities, detect malware and more will be released. DISA plans to award multiple contracts for the project via an enterprise software initiative (ESI) blanket purchase agreement (BPA) in either the third or fourth quarter.

- **Endpoint Security Integration:** An RFP to aid integration of third-party endpoint security tool will be released. DISA plans to award a single contract for the project in the fourth quarter.
- **Global Command and Control System:** An RFP to develop an enterprise system providing Global Common Operational Picture to support defense will be released. DISA plans to award a single contract for the project via a full and open competition in the fourth quarter.
- **Global Video Services (GVS) Engineering, Transition, Implementation and Sustainment Support:** An RFP for video products and transmission types providing full-service video teleconferencing will be released. DISA plans to award a single contract for the project via a small-business set aside in the fourth quarter.

Reference Links

- [DISA Outlines Upcoming Acquisition Opportunities](#)
 - [FORECAST TO INDUSTRY 2019 - AGENDA & BRIEFINGS](#)
-

DISA Seeking Vendors to Build the Unified Situational Cyber Awareness (USCA) Platform

Introduced – September 2019

Summary

The Defense Information Systems Agency is looking for vendors to build a cloud-based enterprise platform that would act as a hub for all cybersecurity operations across the Department of Defense Information Network, or DoDIN. By bringing together the department's disparate cyber capabilities into one place, the platform, called the Unified Situational Cyber Awareness capability, would let personnel rapidly analyze cyber information and coordinate defenses across the department.

Reference Links

- [DISA is Merging Its Cyber Operations Into a Single Cloud-Based Platform](#)
 - [Unified Situational Cyber Awareness \(USCA\)](#)
 - [DISA Looks to Unify Cybersecurity Capabilities](#)
 - [DISA Seeks Contractor to Develop Cyber Situational Awareness Platform](#)
-

DISA, HHS Brainstorming Behavioral-Based Identity Pilot

Introduced – August 2019

Summary

Health and Human Services Department is collaborating with the Defense Information Systems Agency to develop and test using behavioral-based identity at the edge of a network to transform the way people—and particularly, first responders and health officials—log in and secure their work.

Reference Links

- [DISA, HHS Brainstorming Behavioral-Based Identity Pilot](#)
 - [HHS, DISA thinking beyond passwords with network security pilot](#)
-

DISA, Cyber Command Are Launching a Zero-Trust Pilot Program Introduced – August 2019

Summary

The Defense Information Systems Agency is standing up a lab near the agency's Fort Meade headquarters for researchers to test different strategies for building zero-trust network architectures across the Pentagon. Once the lab is operational, security experts from the defense and intelligence communities will use it to experiment with novel approaches to improving identity and access management on military networks

Reference Links

- [DISA, Cyber Command Are Launching a Zero-Trust Pilot Program](#)
-

Department of Energy (DOE)

DOE Announces \$80 Million for New Grid Modernization Lab Call Projects

Introduced – November 2019

Summary

The U.S. Department of Energy (DOE) announced the results of the 2019 Grid Modernization Lab Call with funding of approximately \$80 million over three years. This funding aims to strengthen, transform, and improve the resilience of energy infrastructure to ensure the nation's access to reliable and secure sources of energy now and in the future.

The 2019 Grid Modernization Lab Call is the latest solicitation released over the past four years by the Grid Modernization Initiative (GMI), a crosscutting effort that focuses public and private partnerships to develop a portfolio of new tools and technologies that measure, analyze, predict, protect, and control the grid of the future. This solicitation is focused on developing projects in resilience modeling, energy storage and system flexibility, advanced sensors and data analytics, institutional support and analysis, cyber-physical security, and generation.

Reference Links

- [2019 Grid Modernization Lab Call Awards](#)
 - [Department of Energy Announces \\$80 Million for New Grid Modernization Lab Call Projects](#)
 - [DOE Awards \\$80M to Energy Infrastructure Resiliency Projects](#)
-

DOE Announced Three Projects to Advance Energy Sector Cybersecurity

Introduced – October 2019

Summary

The Department of Energy's (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER) announced awards of nearly \$7 million to support the research, development, and demonstration of next-generation tools and technologies to enhance the cybersecurity of energy delivery systems. Three projects were selected for their merit and potential to enhance the reliability and resilience of the nation's energy infrastructure. The projects will provide energy sector users with tools to assess their cybersecurity posture and help secure operational technology assets.

Reference Links

- [DOE Announces Selections to Advance Energy Sector Cybersecurity](#)
-

DOE and NSF Partner to Launch the National AI Research Institutes Program

Introduced – October 2019

Summary

The National Artificial Intelligence Research Institutes program expects to award approximately \$120 million in 2020 to fund planning and up to six research institutes.

The planning track will provide project up to two years in planning support and \$500,000 for teams to develop communities and capacity for full institute operations. The institute track will support cooperative agreements between \$16 million and \$20 million for four to five years. Each institute will receive up to \$4 million a year. Each institute must have a principal focus on at least one of six themes:

- Trustworthy AI.
- Foundations of machine learning.
- AI-driven innovation in agriculture and the food system.
- AI-augmented learning.
- AI for accelerating molecular synthesis and manufacturing.
- AI for discovery in physics.

Reference Links

- [NSF, Energy Department invest in AI research](#)
 - [National Artificial Intelligence \(AI\) Research Institutes: Accelerating Research, Transforming Society, and Growing the American Workforce](#)
-

Department of Energy Department Launches \$5.5M AI Collaboration

Introduced – October 2019

Summary

The Department of Energy's (DoE) Pacific Northwest National Laboratory (PNNL), its Sandia National Laboratories, and the Georgia Institute of Technology are joining forces in a new artificial intelligence (AI) research center. In a October 2, 2019, press release, DOE revealed that it awarded the institutions \$5.5 million to collaborate on "solutions to some of the most challenging problems in AI today." The center, known as the Center for Artificial Intelligence-

focused Architectures and Algorithms (ARIAA), is funded out of the DoE's Office of Science and will encourage collaboration between the organizations' scientists as they "develop core technologies important for the application of AI to DoE mission priorities." The DoE noted that the scientists will focus on issues such as cybersecurity and electric grid resilience.

Reference Links

- [Energy Department Launches \\$5.5M AI Collaboration](#)
 - [DOE Invests Again in AI](#)
 - [Energy Department creates new AI research center](#)
-

DOE Announced Public-Private Partnerships to Accelerate AI Development

Introduced – October 2019

Summary

During the DOE's fourth InnovationXLab Summit, it announced plans to award up to \$50 million in funding to advance research, development, and the adoption of AI technologies. \$35 million of the announced funding will be distributed through the DoE's Advanced Research Projects Agency-Energy to reduce expenses and increase flexibility in the operation of nuclear plants. Additionally, up to five projects will benefit from \$13 million in funding set to be distributed by the Office of Science. The projects will focus on enhancing the use of AI technologies for scientific investigation and prediction. The project will unite scientists from nine research institutions which include DoE national laboratories and universities.

Reference Links

- [New DoE funding to accelerate AI partnerships with the private sector](#)
-

DOE Establishing Office for Artificial Intelligence and Technology

Introduced – September 2019

Summary

The DOE Artificial Intelligence and Technology Office (AITO) will serve as the coordinating hub for the Artificial Intelligence work being done across the DOE enterprise. Currently, AI is being leveraged by the DOE to strengthen our national security and cybersecurity, improve grid resilience, increase environmental sustainability, enable smarter cities, improve water resource management, as well as

speed the discovery of new materials and compounds, and further the understanding, prediction, and treatment of disease.

Reference Links

- [Secretary Perry Stands Up Office for Artificial Intelligence and Technology](#)
 - [Rick Perry Announces Establishment of DOE Artificial Intelligence Office](#)
-

DOE Seeking Comment on Revised Cybersecurity Capability Maturity Model (C2M2)

Introduced – September 2019

Summary

The Department of Energy has issued for comment revisions to its Cybersecurity Capability Maturity Model (C2M2). C2M2 will focus on implementing cybersecurity practices across organizations, as well as manage those practices. The cybersecurity practices from C2M2 will be associated with information, IT, and operations technology. The updated model will be used to:

- Strengthen cybersecurity;
- Allow for consistent evaluation and benchmarking of cybersecurity capabilities;
- Allow agencies to engage in information and best practice sharing to improve cybersecurity; and
- Enable prioritization of different actions and investments for cybersecurity improvement across agencies.

Reference Links

- [DOE seeks comment on revised cybersecurity 'maturity' model](#)
 - [Energy Updates Cybersecurity Maturity Model](#)
-

DOE Seeking Input on Draft of Latest Cybersecurity Risk Assessment Model

Introduced – August 2019

Summary

The Energy Department is seeking input from industry to update the Cybersecurity Capability Maturity Model designed to help organizations assess their cybersecurity posture. The C2M2 framework was established in 2012 as an open-source model to help fortify the security of the electric grid. DOE used its interviews with industry experts as well as best practices cited in the National Institute of Standards and Technology's most recent cybersecurity framework to inform the development of the latest C2M2 iteration. Interested parties may submit feedback on the new model through Sept. 13.

Reference Links

- [DOE Releases Draft of Latest Cybersecurity Risk Assessment Model](#)
 - [Energy Updates Cybersecurity Maturity Model](#)
-

Federal Communications Commission

FCC bans Chinese telecoms Huawei and ZTE from access to federal broadband subsidies

Introduced – November 2019

Summary

The Federal Communications Commission banned wireless providers from using federal subsidies to purchase any equipment or services from Chinese technology companies Huawei and ZTE.

The agency's unanimous 5-0 vote concluded the two Chinese telecom giants pose a threat to national security and blocked them from receiving any money from the U.S. government's \$8.5 billion Universal Service Fund. The fund subsidizes building broadband infrastructure to increase internet access across the United States in underserved areas.

Reference Links

- [November 2019 Open Commission Meeting](#)
 - [FCC bans Chinese telecoms Huawei and ZTE from access to federal broadband subsidies](#)
-

Federal Election Commission

OIG Finds that FEC Lacks Adequate Information Security Procedures

Introduced – November 2019

Summary

According to an FEC Office of Inspector General (OIG) report released on Nov. 19, 2019, the Federal Election Commission (FEC) is missing effective IT governance and struggles with internal cyber vulnerabilities.

Reference Links

- [Major Management and Performance Challenges Facing the FEC for FY 2020](#)
 - [FEC Lacks Adequate Information Security Procedures, OIG Says](#)
-

Government Accountability Office (GAO)

GAO Identified Cybersecurity Risks to the Electric Grid

Introduced – October 2019

Summary

At the request of Congress, the GAO reviewed the cybersecurity of the electric grid to determine the risks and challenges facing the grid, to describe federal efforts to address those risks, to assess the extent to which the Department of Energy (DOE) has defined a strategy for evaluating grid cybersecurity risks and challenges, and to assess the extent to which Federal Energy Regulatory Commission (FERC)—approved cybersecurity standards address grid cybersecurity risks. GAO recommended that the DOE’s strategy for the grid address the key characteristics of a national strategy, including a full assessment of the cybersecurity risks . The GAO recommendations to FERC included considering adoption of changes to its cybersecurity standards to more fully address the National Institute of Standards and Technology (NIST) Cybersecurity Framework. The second recommendation was to evaluate the potential risk of a coordinated cyber-attack on geographically distributed targets and determine if changes are needed in the threshold for mandatory compliance with the requirements in the full set of cybersecurity standards.

Reference Links

- [CRITICAL INFRASTRUCTURE PROTECTION: CRITICAL INFRASTRUCTURE PROTECTION Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid](#)
 - [Cybersecurity and the Electric Grid – New GAO Report Identifies Actions Needed to Address Cybersecurity Risks](#)
 - [GAO Identifies Electric Grid Cyber Risks, Calls for Stronger Strategy to Protect Grid](#)
 - [GAO Tells DOE to Address Cybersecurity as Electric Grid Faces ‘a Million Attacks Every Day’](#)
 - [FERC looks at potential cyberattacks on dispersed grid assets](#)
 - [FERC cybersecurity report identifies 'potential compliance infractions'](#)
-

Department of Homeland Security (DHS)

CISA Announces Cyber Essentials for Small Business

Introduced – November 2019

Summary

The Cybersecurity Infrastructure Security Agency (CISA) recently released a set of best practices for small businesses. These Cyber Essentials, according to CISA, are intended as a starting point to nurture a “culture of security, and specific actions for leaders and their IT professionals to put that culture into actions.” The Cyber Essentials provide guidance for both organization leaders and IT professionals across six elements:

- Yourself
- Your Staff
- Your Systems
- Your Surroundings
- Your Data
- Your Actions under Stress.

Each element, in turn, provides a number of “Essential Actions” expected of either leaders or IT professionals.

Reference Links

- [Covering the Basics: CISA Announces Cybersecurity Essentials for Small Business](#)
 - [Cyber Essentials](#)
-

CISA invests in election auditing tool to secure 2020 elections

Introduced – November 2019

Summary

DHS’s Cybersecurity and Infrastructure Security Agency (CISA) announced it would partner with election officials and private sector groups to develop an election auditing tool that can be used to help ensure the accuracy of votes in 2020.

CISA is partnering with the non-profit group VotingWorks on an open-source software tool known as Arlo, which is provided to state and local election officials for free. Arlo conducts an audit of votes by selecting how many ballots and which ballots to audit and comparing the audited votes to the original count.

Reference Links

- [DHS cyber agency invests in election auditing tool to secure 2020 elections](#)
 - [EXCLUSIVE: CISA plans post-election audit tool](#)
 - [House Panel Zeroes in on Election Security Ahead of 2020](#)
-

DHS Seeking Feedback on Vulnerability Disclosure Program

Introduced – September 2019

Summary

The Homeland Security Department is seeking feedback on an enterprise-wide vulnerability disclosure program where security researchers can submit weaknesses they uncover in the agency's IT infrastructure without fear of punishment. The effort would bring the department up to speed with the Pentagon and General Services Administration's tech office, which have both already established vulnerability disclosure policies.

Reference Links

- [DHS Asks for Feedback on Vulnerability Disclosure Program](#)
-

CISA Indicates Plans to Fortify U.S. Election Infrastructure

Introduced – September 2019

Summary

Among its "strategic vision and operational priorities" in the recently released [Strategic Intent](#) position paper, CISA indicated an intent to circumvent the Congressional gridlock on election security. Additionally, the agency listed its top five priorities as:

- China, with an emphasis on supply chain management and 5G networks.
- Election security.
- Soft target security.
- Federal cybersecurity.
- Industrial control systems.

Reference Links

- [DHS Cyber Agency Vows to Fortify U.S. Election Security](#)
-

DHS Establishing Transatlantic Aviation Industry Roundtable Committee to Bolster Aviation Cybersecurity

Introduced – September 2019

Summary

The Homeland Security Department is standing up a new committee—the Transatlantic Aviation Industry Roundtable—to engage all relevant flight stakeholders and address critical security issues and threats in the aviation space. Members of the group, who will be appointed by the agency’s secretary and serve applicable terms, will collaborate on a wide variety of issues targeting the transatlantic flight landscape, including global security improvements, information sharing, insider threats, cybersecurity and enhancements to security technologies, among others.

Reference Links

- [Homeland Security Stands Up Transatlantic Aviation Roundtable](#)
 - [DEPARTMENT OF HOMELAND SECURITY: Transatlantic Aviation Industry Roundtable Committee](#)
-

DHS Updating Automated Indicator Sharing Program

Introduced – September 2019

Summary

In the near future, DHS may be updating the Automated Indicator Sharing program, which facilitates the sharing of threat indicators between the federal government and private sector, to better engage with stakeholders and to facilitate increased information sharing.

Reference Links

- [DHS looks to upgrade flagging info sharing program](#)
-

DHS Plans Fall Launch of New Continuous Diagnostics and Mitigation Dashboard

Introduced – September 2019

Summary

The goal of the new dashboard, which has been in development since May 2019, is to give agency IT leaders greater awareness of cybersecurity vulnerabilities and how their IT security compares to that of

other agencies. Starting Oct. 1, agencies that have access to the new dashboard will be able to compare their cybersecurity risk scores, known as Agency-Wide Adaptive Risk Enumeration (AWARE) risk-scoring algorithm. AWARE measures how agencies are doing on basic security practices like vulnerability, patch and configuration management in near real time, where a smaller cumulative score represents a smaller cyberattack surface.

Reference Links

- [DHS Preps New CDM Cybersecurity Dashboard for a Fall Launch](#)
-

DHS Considering Changes to Staff Management for Security Operations Centers Introduced – September 2019

Summary

The Department of Homeland Security is considering shifting how it manages staffing for its 17 Security Operations Centers. The agency wants to move to a single, multiple-award contract vehicle for its SOC. The contract vehicle being contemplated in the RFI would centralize the pool of vendors and create a single set of core functions available to all SOC, which would include:

- Network Monitoring and Security Event Analysis
- Email Security Monitoring and Analysis
- Computer Security Incident Response and Management
- Vulnerability Assessment
- Security Engineering
- Cyber Intelligence Support
- Intrusion Analysis
- Continuity of Operations for SOC Services

Reference Links

- [DHS May Change How It Manages All Its Security Operations Centers](#)
-

Department of Justice (DOJ)

The FBI and DOJ Opened \$100m Idaho Data Centre Hub

Introduced – November 2019

Summary

On Nov. 18, 2019, the FBI and its partners at the Department of Justice (DOJ) participated in a ribbon-cutting ceremony for a new data center at the FBI's facility in Pocatello, Idaho. The new data center will optimize infrastructure, information, and services by consolidating almost 100 data centers throughout DOJ. The consolidation of dozens of data centers will strengthen the cybersecurity posture for all DOJ components using the facility. It will also enhance collaboration, information sharing, and the ability to execute advanced analytics. The new data center will provide the flexibility needed to focus on and rapidly respond to mission requirements.

Reference Links

- [FBI Cuts Ribbon for New Data Center in Idaho](#)
 - [The FBI and DOJ opens \\$100m Idaho data centre hub](#)
-

DOJ Launches the Transnational Elder Fraud Task Force

Introduced – June 2019

Summary

The Justice Department announced the Transnational Elder Fraud Task Force aimed at mitigating foreign-based schemes that target U.S. senior citizens. The task force will encompass DOJ's Consumer Protection Branch, six U.S. attorneys' offices, the FBI and the Postal Inspection Service. It will also work with the Federal Trade Commission. Officials say they'll use data analytics to target frauds ranging from door-to-door cheats to phony online lotteries.

Reference Links

- [Justice Department creates task force to help find schemes targeting seniors](#)
-

General Services Administration (GSA)

GSA and DLA Streamlining the Federal Supply Chain

Introduced – October 2019

Summary

The General Services Administration and the Defense Logistics Agency have partnered to review and streamline the federal supply chain. The DLA-GSA federal supply class review would tackle the 7 million items from across all 600 FSC categories. DLA and GSA are also jointly developing a tool designed to automate data processing on all federal supplies. The tool would help the federal government determine supplies suitable for logistics transfer. Representatives from both agencies will then analyze these items to decide whether a change of logistics approach would streamline the supply chain.

Reference Links

- [DLA, GSA to Review Federal Supply Chain for Streamlining Effort](#)
-

GSA and Air Force Preparing for 5G Rollout

Introduced – October 2019

Summary

At an event hosted by GSA and the Advanced Technology Academic Research Center, Bill Zielinski, assistant commissioner of the General Services Administration's Office of Information Technology Category and rank Konieczny, the U.S. Air Force's chief technology officer discussed how agencies could begin leveraging 5G technology. Zielinski said that testing activities should already begin as the government expects to see a significant increase in mobile data in 2024. Konieczny added that the Air Force plans to expand LTE connectivity to a maximum of 17 bases next fiscal year.

Reference Links

- [Agencies Offer Sneak Peeks into Their 5G Plans](#)
 - [GSA looks to usher in 5G era amid projected surge in agencies' mobile data](#)
 - [GSA, Air Force Officials Seeking Preparations for 5G Rollout](#)
-

Department of Health and Human Services (HHS)

HHS, DISA Aim to Protect Healthcare Data with Assured Identity Pilot

Introduced – November 2019

Summary

The Department of Health and Human Services (HHS) is developing biometric and behavior-based authentication for employees in partnership with the Defense Information Systems Agency (DISA).

Reference Links

- [HHS Explains its Biometric Identity Login Partnership With DISA](#)
 - [HHS, DISA Assured Identity pilot aims to protect healthcare data with biometrics and behavior authentication](#)
-

HHS to Develop Cybersecurity Development Approaches

Introduced – October 2019

Summary

The Department of Health and Human Services is looking to develop unique approaches in incorporating humans into cybersecurity development. Janet Vogel, chief information security officer at the Department of Health and Human Services, said the agency has built an "escape room" that will allow participants to optimize cybersecurity development efforts as part of the National Cybersecurity Awareness Month. The escape room features various cybersecurity challenges and questions and the participants are tasked to complete challenges at every station.

Reference Links

- [HHS to Develop Cybersecurity Dev't Approaches](#)
-

HHS Issued Proposed Rule to Update Anti-Kickback Statute Safe Harbors

Introduced – October 2019

Summary

The Department of Health and Human Services released a Proposed Rule that would modify several existing safe harbors under the Anti-Kickback Statute (AKS) and create a host of new

safe harbor protections. The Proposed Rule seeks to create a safe harbor to protect donations of certain cybersecurity technology and related services. HHS believes that this proposed safe harbor could help improve the healthcare industry's cybersecurity by promoting increased security for interconnected and interoperable healthcare information technology systems without protecting arrangements that either serve as marketing platforms or inappropriately influence clinical decision-making. This change would allow entities to donate cybersecurity software to customers or referrals sources. CMS is proposing a similar exception to the Stark Law. This safe harbor would not be restricted to VBE participants and could be utilized by manufacturers and others.

Comments on the Proposed Rule are due seventy-five (75) days after publication – by December 31, 2019.

Reference Links

- [HHS Issues Proposed Rule to Update Anti-Kickback Statute Safe Harbors – What Does it Mean for Life Sciences Companies?](#)
 - [HHS Anti-Kickback Proposal Features 3 Key Safe Harbors](#)
-

National Institute of Standards and Technology (NIST)

GSA and NIST Working to Automate FedRAMP Assessments

Introduced – November 2019

Summary

The General Services Administration and National Institute of Standards and Technology are working to implement automation in review procedures for the Federal Risk Authorization and Management Program. The two agencies aim to establish a common Open Security Controls Assessment Language to support the integration of automated technologies in vetting operations. GSA is currently seeking input on its OSCAL baseline requirements for FedRAMP compliance and is slated to release a draft of its system security plan guidance by the year's end.

Reference Links

- [GSA, NIST Working to Automate FedRAMP Assessments](#)
 - [GSA, NIST look at automation to remove FedRAMP certification hurdles](#)
-

NIST Partners with Microsoft on Enterprise Patch Management Guidance

Introduced – October 2019

Summary

NIST has partnered with Microsoft to release “The Critical Cybersecurity Hygiene: Patching the Enterprise Project,” a guide intended to ease enterprise patch management. The final publication will be a NIST Cybersecurity Practice Guide, which will be made available to the public. The project is currently seeking technology vendors to participate in the development of an example solution.

Reference Links

- [Critical Cybersecurity Hygiene: Patching the Enterprise](#)
 - [National Cybersecurity Center of Excellence \(NCCoE\) Critical Cybersecurity Hygiene: Patching the Enterprise Building Block](#)
 - [Microsoft and NIST Team Up on Patching Guide](#)
 - [NIST & Microsoft partner for patching pointers](#)
-

NIST Offers a Vendor-neutral Overview of Zero Trust Architecture

Introduced – October 2019

Summary

The [Draft NIST Special Publication 800-207: Zero Trust Architecture](#) offers enterprise network architects, network admins, and cybersecurity admins (with a focus around unclassified civilian networks) a few different things: a simple explanation of what zero trust is, the architectural components needed, use cases, threats to consider, and how to plan a deployment.

Reference Links

- [Draft NIST Special Publication 800-207: Zero Trust Architecture](#)
 - [NIST offers a handy vendor-neutral overview of zero trust architecture](#)
 - [NIST, State Dept Eyeing Zero-Trust Approach to Cybersecurity](#)
 - [NIST to test federal 'zero trust' security architectures](#)
-

NIST Seeking Vendor Insight on Mitigating Risk to Telehealth Cybersecurity

Introduced – September 2019

Summary

NIST wants vendors to provide insight and demonstrations to support the National Cybersecurity Center of Excellence's health care sector-specific use case, "Securing Telehealth Remote Patient Monitoring Ecosystem." In specific, they are seeking input from vendors who can deliver technical expertise and products that can help secure health organizations' telehealth capabilities.

Reference Links

- [NIST Wants Insight on Combatting Telehealth Cybersecurity Risks](#)
 - [NIST: National Cybersecurity Center of Excellence \(NCCoE\) Securing Telehealth Remote Patient Monitoring Ecosystem](#)
 - [NIST Seeks Feedback on Shoring up Telehealth, RPM Cybersecurity Risks](#)
-

NIST Seeking Comments on Improving Health Information Protections

Introduced – September 2019

Summary

The National Institute of Standards and Technology is requesting comments to help providers and other healthcare organizations protect individual privacy. The agency also has issued a preliminary draft on tools to improve privacy through enterprise risk management processes, following a year of public conversations with stakeholders.

Reference Links

- [NIST seeks comments on better protecting health information](#)
-

NIST Soliciting Public Input on Personal Privacy Protections

Introduced – September 2019

Summary

The National Institute of Standards and Technology is looking for feedback on the latest version of a privacy framework meant to help both government and industry manage the risks of holding customers' personal data. The ultimate goal of the framework is to standardize the language around privacy and let leaders in government and industry clearly communicate potential risks and solutions. The public can submit their input on the latest version through Oct. 24.

Reference Links

- [NIST Wants Public Input on Protecting Personal Privacy](#)
 - [NIST requests comments on draft privacy framework](#)
-

NIST Seeking Comment on IoT Cybersecurity Baseline

Introduced – September 2019

Summary

In "[A Starting Point for IoT Device Manufacturers](#)" the National Institute of Standards and Technology (NIST) sought to provide Internet of Things (IoT) device manufacturers a better understanding of appropriate cybersecurity features for the vast and constantly proliferating range of IoT devices.

Reference Links

- [NIST Unveils IoT Baseline of Core Cybersecurity Features for Comment](#)
-

NIST Drafts Security Recommendations for IoT Devices

Introduced – August 2019

Summary

The National Institute of Standards and Technology (NIST) has released a “Core Cybersecurity Feature Baseline for Securable IoT Devices, Draft NISTIR 8259” guide that offers recommendations for what IoT devices should do and what security features they should possess. It is not a set of rules for manufacturers to follow. Rather, it is voluntary guidance intended to help promote the best available practices for reducing risks to IoT security. It complements the recent publication of Considerations for Managing Internet of Things Cybersecurity and Privacy Risks (NISTIR 8228), which primarily addresses large organizations that have more resources to dedicate to IoT cybersecurity.

Reference Links

- [Core Cybersecurity Feature Baseline for Securable IoT Devices: A Starting Point for IoT Device Manufacturers](#)
 - [NIST Drafts Security Recommendations for IoT Devices](#)
 - [NIST seeks industry feedback as Internet of Things cybersecurity standards take shape](#)
-

NIST Delays Cyber Standards for Pentagon Contractors

Introduced – August 2019

Summary

The National Institute of Standards and Technology has delayed the release of cybersecurity standards, NIST Special Publication 800-171, Revision 2, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations," used by Defense Department contractors, pending the review cycle completion of SP 800-53 by Office of Management and Budget, Office of Information and Regulatory Affairs due to dependencies on SP 800-53.

Reference Links

- [NIST delays cyber standards for Pentagon contractors pending OMB review](#)
-

NIST Developing AI Standards

Introduced – August 2019

Summary

The National Institute of Standards and Technology has issued a plan for federal engagement in developing standards and tools to ensure U.S. leadership in artificial intelligence technology, which calls for a process whereby systems can be tested for attributes that contribute to cybersecurity.

Reference Links

- [NIST issues plan for AI standards that includes testing related to cybersecurity](#)
-

National Security Agency (NSA)

NSA Publishes Advisory Addressing Encrypted Traffic Inspection Risks

Introduced – November 2019

Summary

The National Security Agency (NSA) published an advisory that addresses the risks behind Transport Layer Security Inspection (TLSI) and provides mitigation measures for weakened security in organizations that use TLSI products.

Reference Links

- [MANAGING RISK FROM TRANSPORT LAYER SECURITY INSPECTION](#)
 - [NSA Publishes Advisory Addressing Encrypted Traffic Inspection Risks](#)
-

NSA's Cyber Directorate to Focus on Industrial Base

Introduced – October 2019

Summary

Gen. Paul Nakasone, NSA director, said he gave the agency and the directorate, the initial task of securing the defense industrial base and defense weapons systems as it begins to address the demanding challenge of preventing and eradicating cyber-threats to national security systems and critical infrastructure.

Reference Links

- [New NSA cyber directorate to focus on industrial base](#)
-

NSA Reorganizing in Anticipation of the Launch of the New Cybersecurity Directorate

Introduced – September 2019

Summary

The National Security Agency's new cybersecurity directorate will reach initial operating capability (IoC) on October 1, 2019, and full operational capability (FoC) on December 31, 2019. In the meantime, NSA is reorganizing some of its mission areas to fit better under the new directorate. Some of the benefits of the reorganization are increased collaboration, greater offensive and defensive capabilities, increased threat intelligence sharing, and an increased focus on nation state adversaries.

Reference Links

- [New cyber directorate reorgs to help NSA shift focus on nation state adversaries](#)
 - [Leader of new NSA Cybersecurity Directorate outlines threats, objectives](#)
-

NSA Creates New Cybersecurity Directorate

Introduced – August 2019

Summary

The National Security Agency is combining its foreign intelligence and cyber defense missions into a new cybersecurity-focused directorate. The Cybersecurity Directorate will better position the agency to collaborate with partners across the government like U.S. Cyber Command and the Department of Homeland Security, while also enabling them to better share information with industry and agencies. Anne Neuberger, the assistant deputy director of NSA's Operations Directorate, will lead the new directorate. The office will reach initial operating capability by Oct. 1.

Reference Links

- [NSA creates new Cybersecurity Directorate](#)
-

Office of Management and Budget (OMB)

OMB to name agency to lead federal IT supply chain information sharing effort

Introduced – November 2019

Summary

Federal Chief Information Security Officer Grant Schneider said that the administration is in the process of composing the executive branch information-sharing team and determining how it will work with the to-be-named coordinating agency. One goal is for the government to learn more about how it collects and shares IT-related supply chain information among and outside of executive branch agencies.

Reference Links

- [OMB to name agency to lead federal IT supply chain information sharing effort](#)
-

OMB Updates FISMA Guidance for FY2020

Introduced – November 2019

Summary

The Office of Management and Budget released its updated guidance for complying with the Federal Information Security Modernization Act of 2014 (FISMA), setting the timeline for Federal agencies to assess their cybersecurity posture.

The guidance, dated November 19 and addressed to agency leaders, notes that FISMA audits will be required by October 31, 2020, and annual FISMA reports must be submitted to Congress by March 2, 2020. The memo also addresses privacy requirements and management of privacy risks, including reporting requirements for senior agency officials for privacy; requirements for reporting on cybersecurity incidents including what constitutes a major incident that requires additional disclosures, including reporting to Congress; and strengthening continuous diagnostic and mitigation capabilities.

Reference Links

- [MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES](#)
- [OMB Updates FISMA Guidance for FY2020](#)
- [FISMA Compliance Guidance Issued](#)

- [OMB Issues Updated Guidance for Federal Info Security Compliance](#)
-

OMB Opens TIC Policy, Allows Agencies Wider Use of Cloud Services

Introduced – September 2019

Summary

The Office of Management and Budget released the final Trusted Internet Connections (TIC) policy that opens the door much wider to use cloud services. The memorandum provides an enhanced approach for implementing the TIC initiative that provides agencies with increased flexibility to use modern security capabilities and it establishes a process for ensuring the TIC initiative is agile and responsive to advancements in technology and rapidly evolving threats.

Reference Links

- [After a dozen years, agencies are freed from restrictive cyber policy](#)
 - [Update to the Trusted Internet Connections \(TIC\) Initiative](#)
-

Office of Personnel Management (OPM)

OPM Launching Rotational Program for Cyber Reskilling Academy Graduates

Introduced – October 2019

Summary

OPM is working with the Federal CIO Council to create a job rotation program for federal employees who went through the Federal Cybersecurity Reskilling Academy. The rotational program is expected to last for nine months, and complement the three months of academy training. According to OPM's principal associate director for employee services, Veronica Villalobos, "[The] job rotation would provide an opportunity where agencies can be exposed to their work and we figure out how they can be a productive fit within the different CIO shops."

Reference Links

- [OPM to launch job rotation program for cyber reskilling academy graduates](#)
-

Pentagon

Pentagon Developing JEDI Cloud Deployment Security Guidance

Introduced – October 2019

Summary

The Department of Defense is drafting cloud deployment security guidance rooted in zero trust for agencies that will eventually move to the Joint Enterprise Defense Infrastructure cloud.

Reference Links

- [Pentagon developing JEDI cloud deployment security guidance](#)
-

Pentagon 'Hack the Proxy' Programme Uncovered 31 Vulnerabilities

Introduced – October 2019

Summary

During the Pentagon's Hack the Proxy programme on the HackerOne platform, ethical hackers found 31 vulnerabilities – one rated critical while nine got a high severity rating.

Reference Links

- [Pentagon 'Hack the Proxy' programme uncovers 31 vulnerabilities, one critical](#)
 - [DOD Concludes 'Hack the Proxy' Ethical Hacking Effort](#)
-

US Air Force Modernizes Nuclear Weapons Management System

Introduced – October 2019

Summary

The US Air Force has finally modernized the US Strategic Automated Command and Control System (SACCS) away from the floppy disks it was using to manage the US nuclear arsenal, to a "highly-secure solid state digital storage solution."

Reference Links

[US stopped using floppy disks to manage nuclear weapons arsenal](#)

Joint AI Center Soliciting Broad Cybersecurity Pitches

Introduced – July 2019

Summary

Until July 26, 2019, the Joint AI Center is accepting 100 word proposals for cyber and information warfare. Companies whose ideas are accepted may be invited to make “short technical presentations” at an industry day to be determined in the near future.

Reference Links

- [Tell Joint AI Center Your Cyber Defense Idea — In 99 Words Or Less](#)
 - [DOD’s artificial intelligence center wants pitches from industry this fall](#)
-

Department of Veterans Affairs

GAO Finds VA Still Needs to Address Cybersecurity Issues

Introduced – November 2019

Summary

The Government Accountability Office has found that the Department of Veterans Affairs still faces multiple cybersecurity challenges in the course of modernization.

The GAO found that VA must implement security controls to protect sensitive information, identify cybersecurity workforce needs, manage information technology supply chain risks and address known vulnerabilities. The department exhibited a lack of performance in financial reporting security reporting during fiscal year 2018, with deficiencies in access control, configuration management, contingency planning and other areas.

VA met six of 10 administration-imposed cybersecurity goals and holds one of 18 agency information security programs that inspector generals identify as ineffective. A total of 46 GAO-issued recommendations still remain unaddressed by VA.

Reference Links

- [GAO: VA Still Needs to Address Cybersecurity Issues](#)
 - [Watchdog Agencies Report on VA Privacy, Security Woes](#)
 - [VA Cyber Falls Under the Microscope in Congress](#)
-

White House

White House Establishes National Quantum Initiative Advisory Committee

Introduced – September 2019

Summary

The National Quantum Initiative Advisory Committee will help direct Federal research and investments into quantum computing. The committee will advise the Federal agencies tasked with implementing the National Quantum Initiative Act signed into law in December. The Secretary of Energy will name to the committee up to 22 members from “industry, universities, Federal laboratories, and other Federal government agencies” and the director of the Office of Science and Technology Policy (OSTP). The advisory committee’s main task will be to support the activities of the Subcommittee on Quantum Information Science, housed within the National Science and Technology Council (NSTC), by providing expertise and making recommendations. The committee also will solicit expertise from the quantum community at large to inform its recommendations.

Reference Links

- [Executive Order on Establishing the National Quantum Initiative Advisory Committee](#)
 - [White House EO Establishes Quantum Advisory Committee](#)
-