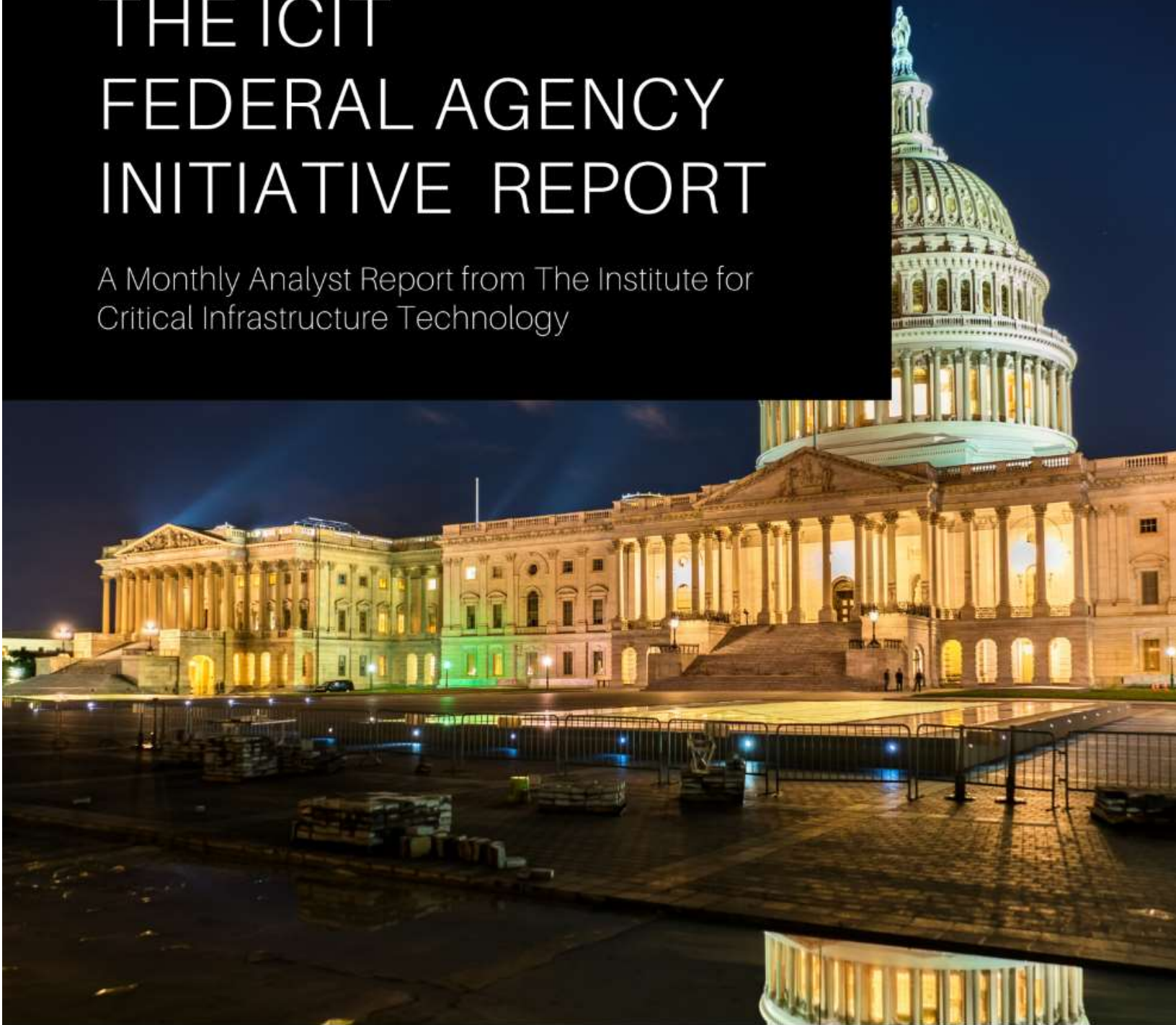


JUNE 2020

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

June 2020

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 2020 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	8
Congressional Initiatives	9
Commissions Lobby for Cyber Personnel Reforms in the Defense Policy Bill	9
Cyberspace Solarium Commission Report May Influence FY 2021 NDAA.....	9
Senate’s Sergeant-at-Arms Soliciting Industry Partner for Insider Threat and Privacy Audits.....	10
Census Bureau	10
Census Bureau Plans to Overhaul Cyber Acquisition Strategy	10
GAO Advises Census Bureau to Address Security and Technology Challenges	11
Census Established a Governance Group on Data Quality Amid COVID-19 Pandemic	11
Census Bureau Seeks Industry Input on Cybersecurity Acquisitions Strategy for Next Decade	12
First Online Census Deployed with Under-tested Platform.....	12
GAO Warns Census 2020 Cybersecurity Issues.....	14
Department of Defense (DOD)	15
GAO Finds Inadequate Security in DOD Key Performance Parameters.....	15
GAO Advises DOD to Address All Requirements of IPv.6 Transition Plan	15
DoD Added Seven 5G Experimentation Sites.....	16
Pentagon Releases 5G Strategy	17
Air Force Space Accelerator Will Nurture Tech Startups Focused on Cybersecurity.....	18
DOD Releases Space Strategy	18
NSA Pilot Providing Secure DNS Services to DOD Agencies and Contractors.....	19
DoD Considers Delaying Chinese Tech Removal Rule Implementation.....	19
Pentagon Plans to Scale Up its Comply-to-Connect Program	20
CMMC Accreditation Body Preps Training Course for DoD Cybersecurity Assessors	21
CMMC won’t apply to commercial-off-the-shelf suppliers	21
DoD’s Proposed Measure to End U.S. Dependency on China for Rare Earth Supplies	21
DoD Developing Standards, Best Practices for AI Initiatives	22
JAIC Highlights Business Process Transformation ‘Mission Initiatives’	22
JAIC Seeking Technical Experts to Develop and Test AI.....	23
Pentagon outlines criteria to pick new HQ for U.S. Space Command	23

DOD Expands Efforts to Secure Mobile Devices	24
GAO Report Finds DoD Cyber-Hygiene Insufficient	24
Pentagon Launches Rumor Control Hub to Dispel Disinformation	24
Some DOD Telework Changes Could be Permanent	25
DARPA VERDICT Tool Aims to Anticipate Military and Industrial Systems Cyber Threats	25
COVID-19 Outbreak May Delay CMMC Audits	26
CMMC Issues RFP for Continuous Monitoring Tool	26
GAO Calls on DoD to Better Track Employee training in its Cyber Awareness Challenge	26
DoD Adopts Ethical Principles for Artificial Intelligence	27
DoD May Require Contractors to Be Cyber-Certified by Fall 2020	27
DoD Issued Warning to Vendors Concerning Fake Third-Party CMMC Certifiers	28
Attacks on DOD Networks Increase in Proportion to Telework Traffic	28
DOD, FBI, and DHS Release Joint Warning of North Korean Threat to Industry	29
DOD to Test How to Secure Satellites from Attack	29
DOD Publishes CMMC Version 1.0	30
Defense Information Systems Agency	31
DISA Disclosed that it Suffered a Data Breach in 2019	31
DISA Streamlining ‘Fourth Estate’ Network Modernization	31
Department of Energy (DOE)	33
DOE and CISA Release Infographic for ICS Cybersecurity	33
DOE Requests \$25 Million to Accelerate ‘Quantum’ Internet Development	33
DOE Announces \$30 Million for Machine Learning and AI Research	33
The Departments of Energy, Homeland Security and Defense Announce Pathfinder Initiative to Protect U.S. Energy Critical Infrastructure	34
DOE Invests \$74M in Building and Construction Technologies	35
DOE Announces \$125.5 Million in New Funding for Solar Technologies	35
Election Assistance Commission (EAC)	36
EAC to Evaluate Cybersecurity, Testing, and Certification of Non-voting Equipment	36
Election Agency Issues Guidance on Handling Primaries and Caucuses During Coronavirus	36
Federal Communications Commission	37
White House's Team Telecom Recommends FCC Block US-Hong Kong Submarine Cable	37
FCC Approves Broadband Deployment in 900 MHz Band	37

GAO Asks FCC to Resolve Cyber Hygiene Issues	38
National Telecommunications and Information Administration Recommends Revoke China Telecom's Common Carrier Status.....	38
FCC To Crack Down On Sharing Of Mobile Users' Location Data	39
Federal Trade Commission (FTC)	40
FTC Delivers Congressional Reports on Consumer Privacy Work.....	40
Government Accountability Office (GAO).....	41
GAO Auditing Expanded Telework and Continuity of Operations Results	41
General Services Administration (GSA).....	42
GSA Issues Guidance to Improve Data Encryption on .gov Sites	42
GSA 18F Project Investigates Factors that Contribute to Modernization Success	42
GSA Awards Funds to Secure 75 Micro Agencies	43
GSA Launches Beta Website for Federal Rulemaking Info	43
GSA Unveils Database for Government-wide Contract Award Info	43
Controls Around the DotGov Program are Tightening	44
GSA Looks to Modernize Approach to Mitigating Fake Public Comments on Rulemakings	44
GSA officials rethink ATO process, workforce reskilling to field AI tools faster	45
GSA, Labor Department Launch AI CoE Project	45
Department of Homeland Security (DHS)	46
CISA Released the First in its Cyber Essentials Toolkit Series	46
Congressional Letter and Internal Report Characterize CIA Cyber-security Controls as "Woefully Lax".....	46
GAO Calls on DHS to Improve Agile Metrics, Training, and Planning	47
CISA Releases Strategy to Improve ICS Cyber-Resiliency.....	48
DHS Warns of Security Issues in Devices from Baxter, BD and Biotronik.....	48
GAO issues chemical facility protection recommendations	48
FBI, CISA Warn of Chinese State-Backed Hackers Targeting COVID-19 Research Orgs.....	49
DHS to Advise Telecom Firms 5G Infrastructure Security.....	50
GAO: DHS Needs More Oversight for Service Contracts	50
DHS CISA and FBI share list of top 10 most exploited vulnerabilities.....	50
CISA Releases Supply Chain Security Resources	51
DHS, NCSC, and CISA Release Joint Advisory on COVID-19 Cyberthreats and Malicious Groups	51
CISA Releases Interim TIC 3.0 Guidance for COVID-19 Telework Surge	52

DHS Categorizes DIB Personnel as “Essential” During the COVID-19 Crisis.....	52
CISA to act as Election Security Liaison Ahead of 2020	53
CISA Releases Election Security Plan Following GAO Criticism	54
DHS Wants to Establish a New Internal Cyber Coordination Group.....	54
DHS CyberOps Center Moving to IT Ops Directorate	55
Department of Justice (DOJ)	56
Revised DOJ Guidance Offers Tightens Risk-management Language	56
DOJ Disrupts Hundreds of COVID-19 Scammer Domains	56
DOJ Launches Coronavirus Cybercrime Task Force	57
DOJ Charges Four Chinese Military Officers in Equifax Breach	57
DOJ Charges Huawei with Racketeering, Illegal Trade with Iran and North Korea	57
Department of Health and Human Services (HHS)	59
HHS Suffers Cyber Incident, Remains Fully Operational	59
National Institute of Standards and Technology (NIST).....	60
NIST Releases Guidance for IoT Device Manufacturers	60
NIST Opens Applications for Digital Forensics Exercise	61
NIST Releases Final Version of SP 1800-23 Guides Identification of Threats to OT Assets	61
NIST Requests Feedback on Digital Identity and Biometric Guidelines	62
NCCoE Designates 10 Tech Partners in Industrial Control System Security Initiative	63
NIST Issues IAST and RASP Guidance	63
NIST Announces Workshop Focused on "Bias in AI"	64
NIST Releases Update for Draft FedRAMP Controls Baseline Guide	64
NIST Invites Industry to Demonstrate 5G-Security Platforms	65
NIST Introduces Framework for Secure Software Development.....	66
NIST Offers Guidance on Evaluating Information Security Monitoring Programs.....	66
NIST Shares Cyber Risk Management, Mobile Guides; Impact Analysis Tool.....	66
NCCoE Soliciting Feedback on “Methodology for Characterizing Network Behavior of Internet of Things” White Paper	67
NIST Considers DevSecOps Framework for Agencies	68
NICE Providing Online Cybersecurity Training Resources.....	68
NIST Seeking Public Comments on Integrating Cybersecurity and Enterprise Risk Management (ERM) Framework	69

NST Offers Telework Security Guidance	69
NIST Releases Roadmap on How to Build Cybersecurity Workforce	70
NIST Releases Tool to Measure the Impact of Supply Chain Risk	71
NIST Releases Draft Guidance on Supply Chain Security	72
NIST seeks comment on ransomware and cyberattack guidance	72
NIST Seeks Industry Support for Data Confidentiality Program	73
Office of Management and Budget (OMB)	75
Auditors Call on OMB to Ensure Agencies Coordinate on State Cybersecurity Requirements	75
OMB Is Clarifying Contracting Language and Security Liability in Cloud SLAs	75
OMB Requests \$45.8B Emergency Funds to Support Telework and Cybersecurity	76
OMB Updates Contracting and Technology Guidance for Federal Agencies	76
Office of Personnel Management (OPM).....	78
37 IGs Report on Agency Tech Challenges Related to \$2.4 Trillion COVID Relief Package	78
OPM Report Highlights Human Capital Management Concerns in Federal Agencies	78
OPM Overhauls Cyber Talent Assessment.....	79
Pentagon	80
Senate Armed Services Committee Tasks Pentagon’s Principal Cyber Advisor with Cyber Pilot Program Responsibilities	80
DARPA Issues Bug Bounty Challenge	80
JAIC set to double its civilian workforce by FY 21 as automation gains momentum	81
JAIC and GSA Reaching out on ‘Discovery Sprint’	81
White House	82
White House signs executive order protecting U.S. bulk power system	82
White House Unveils National Strategy to Secure 5G	82
White House Considering Space Cybersecurity Policies	83
Executive Order instructs agencies to prepare for GPS outage.....	83
White House releases 2021 Budget Proposal	84
Secret Service may rejoin Treasury to improve cybercrime investigations.....	86

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
-

Congressional Initiatives

Commissions Lobby for Cyber Personnel Reforms in the Defense Policy Bill

Introduced – May 2020

Summary

Top leaders from the National Security Commission on Artificial Intelligence, the Cyberspace Solarium Commission, and the National Commission on Military, National, and Public Service signed a joint letter dated May 4 urging top members of the House and Senate Armed Services committees to implement several recommendations to improve the government's attraction, management and retention of cyber professionals. Some recommendations include:

- Expedite the security clearance process,
- Research and develop clearer cyber workforce career paths and leadership roles across government
- Boost funding for the CyberCorps program, a scholarship-for-service program meant as a pathway into the federal cyber workforce

Reference Links

- [Commissions Urge Congress to Enact Federal Personnel Reforms](#)
 - [Commissions lobby for cyber reforms in the defense policy bill](#)
 - [First Cyberspace Solarium Commission Hill hearing today](#)
-

Cyberspace Solarium Commission Report May Influence FY 2021 NDAA

Introduced – April 2020

Summary

Portions of the Cyberspace Solarium Commission Report may be implemented through the upcoming fiscal 2021 National Defense Authorization Act (NDAA). For instance, one consideration would be the creation of a Bureau of Cyber Statistics that would collect and provide statistical data on cybersecurity to inform policymaking and government programs.

The commission – authorized by previous National Defense Authorization Act legislation to study how the U.S. can better defend against cyber threats – issued its signature report last month calling for a harder deterrence strategy, creating cyber-dedicated committees in Congress, establishing a Senate-confirmed National Cyber Director, and strengthening the

Cybersecurity and Infrastructure Security Agency (CISA) to serve as a national cybersecurity coordination hub.

Reference Links

- [Solarium co-chair pushes defense bill as vehicle for implementation](#)
 - [Solarium Officials Press for Cyber Metrics Provisions in NDAA](#)
 - [Cyberspace Solarium Commission getting some of its wishes](#)
-

Senate's Sergeant-at-Arms Soliciting Industry Partner for Insider Threat and Privacy Audits

Introduced – April 2020

Summary

The Senate's sergeant-at-arms is seeking industry assistance with insider-threat and privacy assessments for Senate networks. The SAA wants a vendor to evaluate two aspects of insider threat prevention efforts: SAA's protection of Senate data, which can include personally identifiable information or health data; and assessment of the SAA cybersecurity department's procedures to ensure SAA's data protection efforts can be audited.

Reference Links

- [MARKET SURVEY AND QUALIFIED VENDOR LIST DEVELOPMENT - SOURCES SOUGHT REQUEST FOR CYBERSECURITY SERVICES.](#)
 - [Senate seeks industry's help with internal cyberthreats](#)
-

Census Bureau

Census Bureau Plans to Overhaul Cyber Acquisition Strategy

Introduced – June 2020

Summary

The U.S. Census Bureau is seeking industry input on a new acquisition strategy to revamp its cybersecurity practices over the next decade. The RFI explains that "industry holds the most current and best practices in these areas impacted by cybersecurity," and the agency hopes to use these proven methods to shape its own acquisition strategy. This will "achieve the highest level of cyber defense and resilience" while still following current Federal guidelines.

Reference Links

- [Enterprise Cybersecurity Services Request for Information](#)
 - [Census Seeking to Overhaul Cyber Acquisition Strategy](#)
 - [Census Bureau outlines next 10 years of cybersecurity needs](#)
-

GAO Advises Census Bureau to Address Security and Technology Challenges

Introduced – June 2020

Summary

The GAO reported that the U.S. Census Bureau faces challenges in self-response, operational communication, workforce maintenance, partnerships and other matters amid the COVID-19 pandemic.

GAO advises the bureau to address these and other issues such as homeless individual tracking, information technology risk monitoring, disinformation management and cyber vulnerabilities, the government watchdog said this month in a report to Congress. The report builds on cost and progress reviews of U.S. census efforts this year, with a focus on COVID-19 challenges.

With regard to IT, GAO used official interviews and documented information on the bureau's cybersecurity, IT development, readiness and testing activities for 2020. The 2020 census holds designation as a high-risk program and GAO has issued over a hundred recommendations to address posed risks.

Reference Links

- [COVID-19 Presents Delays and Risks to Census Count](#)
 - [GAO: Census Bureau Faces Multiple Challenges Amid COVID-19](#)
 - [GAO Calls for Renewed Focus on IT, Data, Cyber at Census Amid COVID-19](#)
 - [Census faces pandemic-related delays, cyber and IT challenges](#)
 - [Cyber and IT challenges remain as Census resumes operations](#)
 - [Pandemic could worsen 2020 census IT, cybersecurity challenges](#)
-

Census Established a Governance Group on Data Quality Amid COVID-19 Pandemic

Introduced – June 2020

Summary

In April the Census Bureau stood up a 2020 Data Quality Executive Governance Group to provide guidance on data quality efforts and to facilitate the work of various new and ongoing working groups related to data quality. According to the Bureau, these efforts will identify new ways to assess and ensure quality, security, and privacy both during and after data collection.

Reference Links

- [Census Established a Governance Group on Data Quality Amid COVID-19 Worries](#)
-

Census Bureau Seeks Industry Input on Cybersecurity Acquisitions Strategy for Next Decade Introduced – May 2020

Summary

The U.S. Census Bureau issued a request for information as it decides on acquisitions it might make to improve cybersecurity in a number of areas, such as vendors' ability to provide professional monitoring services for all its technology and information assets "on a 24/7/365 basis," and how it might also leverage emerging technology. The deadline for responding to the Census Bureau's RFI is July 15. The deadline for questions is June 5.

Reference Links

- [Enterprise Cybersecurity Services Request for Information](#)
 - [Census Bureau Seeks Industry Input on Cybersecurity Acquisitions Strategy for Next Decade](#)
 - [Census Bureau Seeks Industry Input to Form Cybersecurity Strategy](#)
-

First Online Census Deployed with Under-tested Platform Introduced – March 2020

Summary

The U.S. Census has been sent out and will be carried out predominantly online, raising concerns about the cybersecurity, data privacy and dips in participation. The platform they will use was never tested fully by the U.S. Census Bureau. When the bureau conducted a "dress rehearsal" for the census in Rhode Island in 2018, it used an entirely different online response platform developed by Pega. Between the Rhode Island test and February test, the bureau abruptly switched to a backup system – an online platform developed in-house called Primus. The bureau had tested the Pega platform to see if it could handle a "stress test" simulation of

600,000 people all trying to fill out their forms at the same time and the platform buckled under the stress. As a result, the bureau switched to the backup system it had been developing in parallel, which officials say can handle the bureau's worst-case scenario of 600,000 people logging in at the same time.

Reference Links

- [Census launches online after last-minute software switch](#)
 - [The 2020 census will take place mostly online. Experts says that raises cybersecurity concerns](#)
 - [The first majority-online census raises novel concerns](#)
-

GAO Warns Census 2020 Cybersecurity Issues

Introduced – February 2020

Summary

The GAO has designated the 2020 Census as a high-risk operation and a recent report noted that the Census Bureau faces “significant cybersecurity challenges in securing its systems and data.” Additionally, the report questioned whether personal data collected during the study can be kept private. GAO noted that the bureau is behind on some of its cybersecurity goals such as recruiting enough workers and addressing the remaining 28 of the 112 recommendations GAO made to secure the 2020 Census.

Reference Links

- [2020 Census: Operations Are Underway with Challenges Remaining](#)
 - [Report Finds Cybersecurity Issues with US 2020 Census](#)
 - [GAO, Congress warn on Census staffing, cyber](#)
 - [Iowa Caucus Meltdown Triggers Talk About Census's New Technology](#)
-

Department of Defense (DOD)

GAO Finds Inadequate Security in DOD Key Performance Parameters

Introduced – June 2020

Summary

The Government Accountability Office assessed the Department of Defense's 121 major defense acquisition programs, information technology procurement and middle-tier acquisition initiatives worth \$1.86T combined and found that DoD did not implement certain measures to achieve its goal of accelerating the delivery of capabilities despite adopting a streamlined approach to acquisition.

In its annual defense acquisition review, the GAO found that the DoD "does not often include cybersecurity" in key performance parameters (KPP) for major programs. Of the three services, the Air Force measured worst at fulfilling two of the three best cybersecurity practices.. The GAO found "inconsistent implementation of leading software practices and cybersecurity measures" among high-dollar "major defense acquisition programs" (MDAPs) — 85 programs worth \$1.80 trillion at the end of 2019. "This included longer-than-expected delivery times for software and delays completing cybersecurity assessments— outcomes disruptive to DOD's efforts to keep pace with warfighters' needs for enhanced, software-dependent capabilities and protect weapon systems from increasingly sophisticated cybersecurity threats,"

Reference Links

- [DEFENSE ACQUISITIONS ANNUAL ASSESSMENT Drive to Deliver Capabilities Faster Increases Importance of Program Knowledge and Consistent Data for Oversight](#)
 - [GAO Chides DoD For Absence Of Cybersecurity Requirements](#)
 - [GAO Releases Annual Assessment of Pentagon's Acquisition Programs](#)
-

GAO Advises DOD to Address All Requirements of IPv.6 Transition Plan

Introduced – June 2020

Summary

The Government Accountability Office (GAO) has advised the Department of Defense (DoD) to address assessment, cost planning and inventory requirements for DoD's transition to the latest version of internet protocol. DoD still needs to identify potential cyber risks and resource and work requirements related to the department's planned transition to IP version six. According

to GAO, so far the DOD has only complied with one of the four requirements imposed by the Office of Management and Budget. The Defense Department has already appointed someone to oversee the transition's planning, but has still not made a complete inventory of IP devices, estimated associated costs and formally analyzed risks, according to GAO.

GAO now recommends DoD's secretary and chief information officer to address the three uncompleted requirements. DoD attempted to pursue IPv6 transition in 2003, 2010 and most recently in 2017.

Reference Links

- [GAO: DoD Must Address All Requirements for IP Transition Plan](#)
 - [Watchdog says Pentagon needs better planning for IP update 17 years after first attempt](#)
-

DoD Added Seven 5G Experimentation Sites

Introduced – June 2020

Summary

The Defense Department is adding seven new installation sites in its second round of 5G technology testing and experimentation. "This latest tranche builds upon DoD's previously announced 5G prototyping and experimentation plan, as well as the recently released Department of Defense 5G strategy," Joseph Evans, DoD technical director of 5G, said Wednesday at the Pentagon via teleconference with reporters. "The bases that were selected were selected for their ability for large scale test facilities to enable rapid experimentation, as well as dual-use application prototyping."

The new bases and their testing specialties consist of:

- Ship-wide/Pier Connectivity at Naval Station Norfolk
- Enhancing Aircraft Mission Readiness at Joint Base Pearl Harbor-Hickam
- Augmented Reality Support of Maintenance and Training at Joint Base San Antonio
- Wireless Connectivity for Forward Operating Bases (FOB) and Tactical Operations Centers (TOC) at the NTC at Fort Irwin and Fort Hood, Texas
- Wireless Connectivity for FOBs and TOCs at Camp Pendleton
- DoD 5G Core Security Experimentation Network at Joint Base San Antonio and multiple remote locations
- Bi-directional Spectrum Sharing between DoD and commercial entities at Tinker Air Force Base

Installation selection criteria included factors such as mature fiber and wireless infrastructure, streamlined access to spectrum bands and prototype, test areas and training range access.

Reference Links

- [DoD expands 5G experimentation sites to 12 installations](#)
 - [New group of DOD sites for 5G testing includes California, Hawaii, Virginia, Texas, Oklahoma](#)
-

Pentagon Releases 5G Strategy

Introduced – June 2020

Summary

The Department of Defense (DoD) has unveiled a new strategy to advance the adoption of secure and resilient 5G networks and stay ahead of potential adversaries.

DoD's 5G Strategy will support national efforts to advance the 5G capabilities of the U.S. and its partners, promote awareness of national security risks posed by 5G and come up with approaches to safeguard 5G technologies and infrastructure to achieve key outcomes, such as having resilient capabilities leveraging ubiquitous connectivity and assured global spectrum access within contested and congested environments.

The strategy has four lines of effort: promote technology development; assess, operate and mitigate through 5G vulnerabilities; influence 5G standards and policies; and engage partners.

To advance technology development, the Pentagon will host 5G industry demonstrations, promote national and international standards with regard to millimetre-wave technologies, pursue the development of technologies needed for real-time spectrum sharing, advance open architecture and virtualization and launch workforce development efforts.

DoD's strategic plan aligns with the Trump administration's National Strategy to Secure 5G and the fiscal 2020 National Defense Authorization Act.

Reference Links

- [Pentagon Releases 5G Strategy](#)
-

Air Force Space Accelerator Will Nurture Tech Startups Focused on Cybersecurity

Introduced – June 2020

Summary

The Air Force Space Accelerator Program has opened the competition for its latest cohort of tech startups, offering to nurture a handful of new companies working cybersecurity in the space sector. There are eight slots available in the new cohort for contest winners, and they get a three-month residency at the Colorado Springs campus of the Catalyst Space Accelerator. The problem proposes using cybersecurity technologies “to secure the next generation of space operations and increase resiliency” of existing systems. It specifically highlights the issue of cyber-physical systems including systems that move satellite antennas or control propulsion.

Reference Links

- [Air Force Space Accelerator Will Nurture Tech Startups Focused on Cybersecurity](#)
 - [#CACSA | Cyber for Space Applications](#)
-

DOD Releases Space Strategy

Introduced – June 2020

Summary

The Department of Defense (DoD) has launched a new strategy that outlines how DoD will advance and leverage space capabilities to compete, deter and counter potential adversaries in the space domain. “This strategy identifies a phased approach on how we are going to achieve the desired conditions in space over the next 10 years,” according to DOD Secretary Mark Esper. He continued, “The Defense Space Strategy is the next step to ensure space superiority and to secure the Nation’s vital interests in space now and in the future.”

The Pentagon has set three objectives to advance space power:

- Maintain space superiority;
- Ensure space stability;
- Provide space support to joint, national and combined operations.

The strategy outlines four lines of effort to address challenges, threats, and opportunities and reach the desired conditions:

- Build a comprehensive military advantage in space;
- Integrate military spacepower into national, joint and combined operations;

- Shape the strategic environment;
- Cooperate with allies, industry, partners, and other U.S. government departments and agencies.

Reference Links

- [DEFENSE SPACE STRATEGY - SUMMARY](#)
 - [DoD Unveils Defense Space Strategy; Mark Esper Quoted](#)
-

NSA Pilot Providing Secure DNS Services to DOD Agencies and Contractors

Introduced – June 2020

Summary

The National Security Agency (NSA) is conducting a pilot program through a commercial managed service provider that provides secure domain-name system (DNS) services to a group of defense industrial base (DIB) companies.

The program stems from a partnership across Department of Defense (DoD) agencies, and is based on NSA analysis that found “using secure DNS would reduce the ability for 92 percent of malware attacks both from command and control perspective deploying malware on a given network.”

Reference Links

- [NSA Pilot Providing Secure DNS Services to DIB](#)
 - [NSA Piloting Secure Domain Name System Service for Defense Contractors](#)
-

DoD Considers Delaying Chinese Tech Removal Rule Implementation

Introduced – June 2020

Summary

A section in the fiscal 2019 National Defense Authorization Act requiring government contractors to remove Chinese-made technologies from their networks is now slated to take effect in August 2020 and the Department of Defense (DoD) is considering delaying by a year full compliance with that provision, DoD fully supports the intent of Section 889, but the Department is hearing that, in light of the COVID impacts and disruptions to the industrial base including small businesses, there may be reasons to extend by one year the implementation of

the rule,” according to Lt. Col. Mike Andrews, on behalf of the DoD. He continued, “While necessary to accomplish, the requirements of 889 will require significant investment and may benefit from use of a risk based approach to achieve effective implementation.”

The Office of Management and Budget (OMB) has yet to issue guidance for contractors to comply with the NDAA provision.

Reference Links

- [DoD Considers Delaying Chinese Tech Removal Rule Implementation](#)
-

Pentagon Plans to Scale Up its Comply-to-Connect Program

Introduced – June 2020

Summary

The Comply-to-Connect (C2C) program ensures devices connecting to military networks have baseline security without needing to install endpoint management apps. The RFI outlines several technical characteristics DISA wants in potential solutions, including:

- A single, converged platform to “discover, identify, categorize, classify and profile all devices” connected to the DODIN. To ensure the platform is a catch-all for everything touching the network, the software must use “the widest variety of both passive and active network-based and host-based discovery methodologies.”
- The ability to “automatically remediate deviations from established required compliance baselines” on non-compliant devices without the need to install endpoint management software on the device.
- The ability to segment networks—or manage segmentation—to block non-compliant devices. Then, once the devices have been updated, “segregate devices by type/function to limit access to only mission necessary network segments.” This capability should also be achieved without the use of an endpoint agent.
- Continuously monitor devices for compliance and ensure information sharing between various cybersecurity components.

Responses are due by 1 p.m. June 26. Questions on the RFI are due by 1 p.m. June 25 and will only be accepted by email.

Reference Links

- [Comply-to-Connect \(C2C\)](#)
 - [Pentagon Wants to Scale Up Its Device Security Program](#)
-

CMMC Accreditation Body Preps Training Course for DoD Cybersecurity Assessors

Introduced – May 2020

Summary

The accreditation body for the Department of Defense's Cybersecurity Maturity Model Certification program is developing a course to train independent assessors who will evaluate contractors' ability to comply with CMMC requirements. Ben Tchoubineh, chair of the CMMC-AB training committee, said the panel expects to kick off the first phase of its course in three to six months and formally launch its program by early 2021.

Reference Links

- [CMMC Accreditation Body Preps Training Course for DoD Cybersecurity Assessors](#)
 - [Pentagon's Cybersecurity Accreditation Board Seeks First Class of Auditors](#)
 - [The CMMC AB's Plan to Train the Assessors](#)
-

CMMC won't apply to commercial-off-the-shelf suppliers

Introduced – May 2020

Summary

A recent change in the FAQ section of the DOD website indicates that The Cybersecurity Maturity Model Certification (CMMC) will not apply to Department of Defense suppliers that only provide commercial-off-the-shelf products.

Reference Links

- [CMMC FAQ's](#)
 - [CMMC won't apply to commercial-off-the-shelf suppliers, DOD website shows](#)
-

DoD's Proposed Measure to End U.S. Dependency on China for Rare Earth Supplies

Introduced – May 2020

Summary

The Department of Defense (DoD) has proposed a measure that seeks to advance direct investments to end the country's dependence on China for rare earth elements used to produce munitions, hypersonic systems, missiles and other defense systems. The proposed bill would increase spending caps under the Defense Production Act to allow DoD to allocate up to

\$1.75B in funds for rare earth minerals for use in missiles and munitions and up to \$350 million for microelectronics.

Reference Links

- [DoD's Proposed Measure Seeks to Allocate Over \\$2B to End U.S. Dependency on China for Rare Earth Supplies](#)
-

DoD Developing Standards, Best Practices for AI Initiatives Introduced – May 2020

Summary

DoD's R&E office is working on a series of best practices and technical standards for its artificial intelligence initiatives amid a rising number of AI efforts spread across the Pentagon

Reference Links

- [DoD developing 'best practices' for AI programs](#)
 - [Mark Lewis: DoD Working on Standards, Best Practices for AI Initiatives](#)
-

JAIC Highlights Business Process Transformation 'Mission Initiatives' Introduced – May 2020

Summary

The Department of Defense's (DoD) Joint Artificial Intelligence Center (JAIC) has detailed its mission initiatives focused on achieving the DoD's business process transformation goals. The AI projects are meant to automate the DoD's digital workloads and "increase productivity at scale". The MIs encompass lines of effort such as acquisition, business administration, customer relations, finance and budget, human capital management and training and development.

JAIC intends to work with entities such as the Washington Headquarter Services and the service branches in a range of technical areas such as machine learning, natural language processing and robotic process automation. Use cases for the proposed initiatives include the deployment of an ML model to detect discrepancies in U.S. Army transactions, RPA-driven U.S. Navy document processing and automated reviews of forms for Office of Management and Budget compliance.

Reference Links

- [JAIC Highlights 'Mission Initiatives' for Business Process Transformation](#)
-

JAIC Seeking Technical Experts to Develop and Test AI

Introduced – May 2020

Summary

In late April the center posted an announcement seeking information on hiring 18-40 “highly technical” contractors who could assist in a range of mission support activities. These contractors would perform systems engineering, cybersecurity and user experience design development, among other tasks.

Reference Links

- [Pentagon’s JAIC on the hunt for technology, technical experts to develop and test AI](#)
 - [Joint Artificial Intelligence Center \(JAIC\) Mission Support](#)
-

Pentagon outlines criteria to pick new HQ for U.S. Space Command

Introduced – May 2020

Summary

US Space Command will stay at its temporary home in Colorado Springs for the next six years. Defense officials outlined a new set of criteria they’ll use to pick SPACECOM’s permanent home.

In a letter to governors, John Henderson, the assistant secretary of the Air Force for installations said the new location would need to be within commuting distance of one of the nation’s biggest 150 metropolitan areas, within 25 miles of a military base, and have a score of at least 50 out of 100 on AARP’s “Livability Index.”

Reference Links

- [Pentagon outlines criteria to pick new HQ for U.S. Space Command](#)
-

DOD Expands Efforts to Secure Mobile Devices

Introduced – May 2020

Summary

The Department of Defense is leveraging automated testing software to secure mobile applications across the military. Additionally, the Defense Information Systems Agency (DISA) is working with the U.S. Air Force to test physical cases designed to bolster the security of mobile devices used by airmen.

Reference Links

- [DOD expands testing of mobile apps with new automated software](#)
 - [DISA, USAF Partner to Bolster Mobile Device Security](#)
 - [Air Force and DISA working to secure off-the-shelf phones with specialized cases](#)
-

GAO Report Finds DoD Cyber-Hygiene Insufficient

Introduced – April 2020

Summary

An April 13 report from Government Accountability Office report, titled "DOD Needs to Take Decisive Actions to Improve Cyber Hygiene," warned that the Pentagon faces increased cybersecurity risk because the department hasn't implemented basic cybersecurity practices.

The watchdog evaluated three Pentagon initiatives: DOD Cybersecurity Culture and Compliance Initiative (DC3I), Cybersecurity Discipline Implementation Plan (CDIP), and cyber awareness training.

Reference Links

- [Watchdog finds the Pentagon is behind on several cybersecurity initiatives](#)
 - [GAO Rakes DoD Over Cyber Hygiene Implementation](#)
 - [GAO: Pentagon's Cyber Hygiene Programs Come Up Short](#)
 - [Pentagon falls short on its cyber hygiene goals, GAO says](#)
-

Pentagon Launches Rumor Control Hub to Dispel Disinformation

Introduced – April 2020

Summary

The Pentagon recently launched an online resource—named Rumor Control—to help quell the myths and incorrect information that have been swirling around the novel coronavirus pandemic.

Reference Links

- [Pentagon Launches Coronavirus Mythbuster Site](#)
-

Some DOD Telework Changes Could be Permanent Introduced – April 2020

Summary

DOD rolled out the CVR or Commercial Virtual Remote environment to handle the deluge of teleworkers March 27. It now has over 900,000 user accounts with 250,000 added per day, according to an April 13 briefing. CVR is a collaboration suite based on Microsoft Teams that enables video, voice and text communications.

Reference Links

- [Some of DOD's telework changes could be permanent](#)
 - [DoD telework capability may outlive pandemic](#)
 - [Pentagon touts massive expansion in IT capability to support telework](#)
-

DARPA VERDICT Tool Aims to Anticipate Military and Industrial Systems Cyber Threats Introduced – April 2020

Summary

The Verification Evidence and Resilient Design in Anticipation of Cybersecurity Threats—or VERDICT—tool aims to work across a range of computer systems, such as those for smart devices, ships, aircraft, power plants and wind farms. The goal is to provide the systems with comprehensive assessments of cyber threats, recommend how to address vulnerabilities uncovered, and predict the potential of forthcoming attacks.

Reference Links

- [DARPA Project Producing Tool to Help Anticipate Military and Industrial Systems' Cyber Threats](#)

- [GE Researchers Working to Improve Cyber Resiliency of Critical Military and Industrial Systems](#)
-

COVID-19 Outbreak May Delay CMMC Audits

Introduced – April 2020

Summary

According to Katie Arrington, the chief information security officer with the Office of the Undersecretary of Defense for Acquisition, the first audits for the Cybersecurity Maturity Model Certification and pathfinder projects could be delayed up to a month due to the coronavirus pandemic, since actual audits must be done on site.

Other reports confirm that plans to train and confirm CMMC third-party assessment organizations, known as C3PAOs remain on track.

Reference Links

- [COVID-19 outbreak may delay audits for DOD's cyber certification](#)
 - [COVID-19 NEWS: New Cybersecurity Regulations 'On Track' Despite Virus](#)
-

CMMC Issues RFP for Continuous Monitoring Tool

Introduced – April 2020

Summary

The accreditation body for the Department of Defense's Cybersecurity Maturity Model Certification program has issued a request for proposals for a continuous monitoring platform that certified third-party assessment organizations, assessors and companies seeking certification can use the continuous monitoring tool to carry out pre-evaluation background research and monitor firms between formal assessments.

Reference Links

- [CMMC Accreditation Body Issues Solicitation for Continuous Monitoring Tool](#)
-

GAO Calls on DoD to Better Track Employee training in its Cyber Awareness Challenge

Introduced – April 2020

Summary

According to the GAO, the Defense Department is not fully tracking employee training in its Cyber Awareness Challenge, a main element of the department's cybersecurity programs. That required training "is intended to help the DoD workforce maintain awareness of known and emerging cyber threats, and reinforce best practices to keep information and systems secure." However, in examining 16 DoD components, GAO found that six lacked information on system users who had not completed the training in 2018, and eight lacked information on users whose network access had been revoked for not completing training.

Reference Links

- [GAO Call on DoD to Better Track Cybersecurity Training](#)
-

DoD Adopts Ethical Principles for Artificial Intelligence Introduced – March 2020

Summary

The U.S. Department of Defense officially adopted a series of ethical principles for the use of Artificial Intelligence following recommendations provided to Secretary of Defense Dr. Mark T. Esper by the Defense Innovation Board last October.

The recommendations came after 15 months of consultation with leading AI experts in commercial industry, government, academia and the American public that resulted in a rigorous process of feedback and analysis among the nation's leading AI experts with multiple venues for public input and comment. The adoption of AI ethical principles aligns with the DOD AI strategy objective directing the U.S. military lead in AI ethics and the lawful use of AI systems.

Reference Links

- [DoD Adopts Ethical Principles for Artificial Intelligence](#)
-

DoD May Require Contractors to Be Cyber-Certified by Fall 2020 Introduced – March 2020

Summary

The CMMC framework contemplates a certification requirement to have a third-party auditor verify that a contractor has implemented the processes and practices associated with a particular cybersecurity maturity level. CMMC requirements are expected to be noted in requests for information concerning government procurements beginning in spring 2020, after which implementing language will be added to the Defense Federal Acquisition Regulation Supplement by summer 2020. New “go/no go” requirements in requests for proposals are expected by fall 2020.

Reference Links

- [DoD to Require Contractors to Be Cyber-Certified by Fall 2020](#)
 - [The future of defense contractor cybersecurity standards](#)
-

DoD Issued Warning to Vendors Concerning Fake Third-Party CMMC Certifiers

Introduced – March 2020

Summary

The DoD finalized the CMMC requirements in January and is still working on the testing mechanisms for accreditation. They warn companies that third-parties that “ensure accreditation” are not being honest with their customers. The accreditation body is considering how to best address the issue and may litigate or send “cease and desist” letters to any company that claims they can get another vendor certified.

Reference Links

- [DoD warns vendors about fake third-party CMMC certifiers](#)
-

Attacks on DOD Networks Increase in Proportion to Telework Traffic

Introduced – March 2020

Summary

Cyber attacks on Defense Department networks increased as teleworking employees put “unprecedented” loads on the military’s computer networks. To protect Defense Department networks, the Pentagon is barring users from accessing YouTube and other streaming services. It’s one of several concerns officials expressed about rapidly moving the federal government’s largest agency toward “maximized telework.”

Reference Links

- [Attacks on DOD Networks Soar as Telework Inflicts ‘Unprecedented’ Loads](#)
 - [DOD faces network attacks amid telework uptick](#)
 - [Pentagon Leaders Stress Cybersecurity As More Personnel Move to Telework](#)
 - [Mass teleworking causes spike in DOD network attacks](#)
-

DOD, FBI, and DHS Release Joint Warning of North Korean Threat to Industry Introduced – February 2020

Summary

The Pentagon, FBI, and Department of Homeland Security have publicly identified a North Korean hacking campaign as part of a broad information sharing program intended to warn industry against adversarial hacking. The public disclosure includes details about at least seven different malware samples linked with North Korean hacking efforts. The samples point to cyber-espionage activities carried out by an actor the U.S. refers to as Hidden Cobra, which officials have previously associated with the North Korean government. The files detailed use tools meant to steal data, create and delete files and capture screenshots.

Reference Links

- [CISA, FBI and DOD Issue Warning on North Korea-Linked Malware](#)
 - [North Korean Malicious Cyber Activity](#)
 - [Pentagon, FBI, DHS jointly expose a North Korean hacking effort](#)
-

DOD to Test How to Secure Satellites from Attack Introduced – February 2020

Summary

A new report from the DOD warns that the military today is not able to assess the durability of its satellites if they came under attack. The DOD plans to invest at least \$100 billion in space systems over the next decade, and it has to be able to test satellites against cyber, directed-energy, kinetic and electronic warfare threats, as well as natural hazards. Director of Operational Test and Evaluation (DOT&E) Behler writes, “This multi-layered space testing and evaluation capability is key to the DoD’s being able to demonstrate the true functionality, limitations, survivability, and employment considerations of space systems.”

Reference Links

- [FY 2019 Annual Report](#)
 - [Pentagon report: DoD needs to test how satellites would perform under attack](#)
 - [Pentagon statement: DoD to perform experiments on how satellites can withstand the attack](#)
-

DOD Publishes CMMC Version 1.0

Introduced – February 2020

Summary

The CMMC model framework organizes processes and cybersecurity best practices into a set of domains. Any company that does business with the Department of Defense, primes as well as subcontractors, must have "at least a basic level of cybersecurity standards" when they respond to requests for proposals.

Reference Links

- [U.S. Department of Defense Publishes New Cybersecurity Standards](#)
 - [A look at CMMC](#)
 - [DoD to Require Cybersecurity Certification From Defense Contractors](#)
-

Defense Information Systems Agency

DISA Disclosed that it Suffered a Data Breach in 2019

Introduced – March 2020

Summary

The Defense Information Systems Agency confirmed that it experienced a data breach between May and July of 2019. DoD spokesman Charles Pritchard confirmed the breach occurred, stating

“While there is no evidence to suggest that any of the potentially compromised personally identifiable information (PII) was misused, DISA policy requires the agency to notify individuals whose personal data may have been compromised. Individuals possibly affected by this incident will receive letters containing initial notification of the situation. They will subsequently receive additional correspondence with information about actions that can be taken to mitigate possible negative impacts. Those actions will include access to free credit monitoring services for all affected by this breach. DISA has conducted a thorough investigation of this incident and taken appropriate measures to secure the network.”

Pritchard did not specify what sort of system was breached or precisely what types of individuals might have been affected — current or former DoD employees, contractors or others.

Reference Links

- [DoD Agency Suffers Data Breach, Potentially Compromising SSNs](#)
 - [DISA exposes personal data of 200,000 people](#)
 - [U.S. DoD Reveals Data Breach Against Defense Information Systems Agency](#)
-

DISA Streamlining ‘Fourth Estate’ Network Modernization

Introduced – February 2020

Summary

The Pentagon is streamlining the look and feel of desktop applications for DOD support agencies. Roughly a fifth of the Defense Department’s budget is devoted to the “fourth estate,” the defense headquarters, support agencies and activities not inside the military departments. For more than a year, the Pentagon has been pushing to consolidate the networks for the fourth estate and is now making progress.

The Defense Information Systems Agency, the DOD's IT services arm, has been working on moving to a new, single-service network called DODNet. DISA has been shifting its own IT support services to the consolidated network and will spend the rest of the year moving the first agencies to it.

Reference Links

- [DISA Makes Progress on 'Fourth Estate' Network Modernization](#)
-

Department of Energy (DOE)

DOE and CISA Release Infographic for ICS Cybersecurity

Introduced – May 2020

Summary

The United States' infographic details common ICS risk considerations and impacts of cybersecurity events. DoE and CISA also provided eight best practices concerning risk management and cybersecurity governance, physical security, host security, security monitoring, ICS network architecture, ICS network perimeter security, supply chain management, and the human element. Each best practice includes actionable steps IT professionals can take to both strengthen their cybersecurity infrastructure and improve cybersecurity culture and hygiene within their organization.

Reference Links

- [U.S., UK Share Best Practices for Infrastructure Cybersecurity](#)
 - [Recommended Cybersecurity Practices for Industrial Control Systems](#)
-

DOE Requests \$25 Million to Accelerate 'Quantum' Internet Development

Introduced – May 2020

Summary

The DOE has requested \$25 million of the Trump administration's 2021 budget request to accelerate the development of a quantum internet. Such a has the potential to reinvent fields including cybersecurity and material science.

Reference Links

- [Trump betting millions to lay the groundwork for quantum internet in the US](#)
-

DOE Announces \$30 Million for Machine Learning and AI Research

Introduced – April 2020

Summary

The U.S. Department of Energy (DOE) announced a plan to provide up to \$30 million for advanced research in machine learning (ML) and artificial intelligence (AI) for both scientific investigation and the management of complex systems.

The initiative encompasses two separate topic areas. One topic is focused on the development of ML and AI for predictive modeling and simulation focused on research across the physical sciences. A second topic is focused on basic ML and AI research for “decision support” in managing complex systems. Potential eventual applications could include cybersecurity, power grid resilience, and other complex processes where ML and AI can make or aid in making decisions in real time.

Reference Links

- [DOE Announces \\$30 Million for Machine Learning and AI Research](#)
 - [Funding Opportunities](#)
 - [Department of Energy Announces \\$30M for Machine Learning and Artificial Intelligence Research](#)
 - [Department of Energy Announces \\$30 Million for Machine Learning and Artificial Intelligence Research](#)
-

The Departments of Energy, Homeland Security and Defense Announce Pathfinder Initiative to Protect U.S. Energy Critical Infrastructure

Introduced – February 2020

Summary

The U.S. Department of Energy (DOE), U.S. Department of Homeland Security (DHS), and U.S. Department of Defense (DoD) jointly signed a Memorandum of Understanding (MOU) to partner on a new Energy Sector Pathfinder initiative. The goals of this initiative are to advance information sharing, improve training and education to understand systemic risks, and develop joint operational preparedness and response activities to cybersecurity threats.

Reference Links

- [U.S. Department of Energy, U.S. Department of Homeland Security, and U.S. Department of Defense Announce Pathfinder Initiative to Protect U.S. Energy Critical Infrastructure](#)
 - [Three agencies team on cyber defense of energy infrastructure](#)
 - [Federal Agencies Come Together to Enhance Cybersecurity in Energy Sector](#)
-

DOE Invests \$74M in Building and Construction Technologies

Introduced – February 2020

Summary

The U.S. Department of Energy (DOE) will award \$74 million to 63 selected projects to research, develop, and test energy-efficient and flexible building technologies, systems, and construction practices to improve the energy performance of the nation's buildings and electric grid.

Crucially, the initiatives are required to address the cybersecurity of flexible buildings and verify the performance of their equipment.

Reference Links

- [DOE Invests \\$74M In Building And Construction Technologies](#)
 - [Department of Energy Invests \\$74 Million in Building and Construction Technologies and Innovations](#)
-

DOE Announces \$125.5 Million in New Funding for Solar Technologies

Introduced – February 2020

Summary

The U.S. Department of Energy (DOE) announced up to \$125.5 million in new funding to advance solar technology research. Through the Office of Energy Efficiency and Renewable Energy (EERE) Solar Energy Technologies Office, DOE continues to advance research and development of solar technologies that reduce the cost of solar, increase the competitiveness of American manufacturing and businesses, and improve the reliability of the grid.

Projects will tackle key emerging challenges facing the solar industry, including enhancing cybersecurity protections, enabling solar and storage, manufacturing, developing solar-powered microgrids, and siting solar with agriculture. Under Secretary of Energy Mark W. Menezes states, "Progress made in cybersecurity and grid integration build on previous FOAs, and including new topics to help the agriculture community and folding in AI technologies and machine learning, only help bolster the need for solar technologies now, and in the future."

Reference Links

- [Department of Energy Announces \\$125.5 Million in New Funding for Solar Technologies](#)
 - [US earmarks US\\$125.5 million of government money for solar R&D](#)
 - [DoE announces \\$125.5 million in solar research funding](#)
-

Election Assistance Commission (EAC)

EAC to Evaluate Cybersecurity, Testing, and Certification of Non-voting Equipment

Introduced – June 2020

Summary

The EAC is taking the first step toward a testing and certification program for e-poll books, results websites, and other election technology not currently covered by federal certification standards. The new pilot project, known as RABET-V, will also seek out ways to encourage manufacturers to design systems for frequent, incremental updates and re-certifications, a major goal of election security experts who criticize the current cumbersome process.

The EAC has partnered with the nonprofit Center for Internet Security on a pilot project to evaluate ways to test and certify non-voting election equipment. Indiana, Maryland, Ohio, Pennsylvania, Texas and Wisconsin are part of the “Rapid Architecture-Based Election Technology Verification” project. So is the Federal Voting Assistance Program, which coordinates voting processes for overseas Americans and U.S. service members, the two largest constituencies for internet voting — another technology currently outside the scope of federal certification.

Reference Links

- [EAC to evaluate testing and certification of non-voting equipment](#)
-

Election Agency Issues Guidance on Handling Primaries and Caucuses During Coronavirus

Introduced – March 2020

Summary

The Election Assistance Commission published a list of resources for state election officials, voting system vendors, and federal agencies on how to deal with the coronavirus.

Reference Links

- [Coronavirus \(COVID-19\) Resources](#)
 - [Election Agency Issues Guidance on Handling Primaries and Caucuses During Coronavirus](#)
-

Federal Communications Commission

White House's Team Telecom Recommends FCC Block US-Hong Kong Submarine Cable

Introduced – June 2020

Summary

The Justice Department-led commission cited Chinese cybersecurity laws in spurning an undersea cable that would vastly improve the speed and capacity of data transfers to the region. Team Telecom, the subject of a recent executive order, is chaired by the Justice Department and includes input from the departments of Homeland Security, Defense, Treasury, State and others.

The newly formed 'Team Telecom' has recommended that the FCC deny the Pacific Light Cable Network System submarine cable connecting the United States to Hong Kong. The 12,800km cable is mostly laid and ready to launch, but has been beset by issues. It was supposed to open in 2018, but has suffered setbacks, as well as changes of ownership - with the four fiber pairs owned by PLDC shifting from Hong Kong steel and property magnate Wei Junkang to China's Dr. Peng Group, a telco company with alleged links to the Chinese state.

Reference Links

- [White House's Team Telecom recommends FCC block US-Hong Kong cable backed by Google, Facebook](#)
- [New Team Telecom Recommendation Doesn't Bode Well for U.S.-China Connections](#)
- [Team Telecom Offers Recommendation to FCC on Pacific Light Cable Network's Application](#)
- [Federal agencies recommend blocking Hong Kong-US undersea cable over national security concerns](#)
- [Agencies say FCC should deny request for underwater cable between Hong Kong and US](#)

FCC Approves Broadband Deployment in 900 MHz Band

Introduced – May 2020

Summary

A portion of the 900 megahertz (MHz) band, which is currently designated for narrowband land mobile radio communications and primarily used by utility, transportation, manufacturing, and

petrochemical companies, will now be available to those industries to develop and deploy critical wireless broadband technologies and services.

Reference Links

- [FCC Opens 900-MHz Band for Broadband Use](#)
 - [FCC gives utilities, other industries green light to deploy broadband in 900 MHz band](#)
-

GAO Asks FCC to Resolve Cyber Hygiene Issues

Introduced – April 2020

Summary

A GAO report looked at the implementation status of 136 information security recommendations from a September 2019 evaluation by the watchdog agency. As of November 2019, it found that the FCC has fully implemented 85 of the recommendations, with 10 partially implemented and another 41 not addressed. Key steps that the FCC must take include resolving known vulnerabilities, applying security patches and improving network-monitoring capabilities. For instance, as of April 24, The Federal Communications Commission still has data flowing through its network without proper encryption.

The FCC is in the process of correcting basic cybersecurity shortfalls, like properly protecting data, giving IT systems proper authorization to operate and speeding up incident response. According to the GAO, the FCC has created action plans to address the remaining recommendations by April 2021.

Reference Links

- [Watchdog says FCC must address basic cyber hygiene issues](#)
 - [Federal watchdog finds cybersecurity vulnerabilities in FCC systems](#)
 - [FCC needs to fix its cybersecurity practices, GAO finds](#)
 - [Three Years Post-Disruption, FCC Still Hasn't Started One-Third of GAO Cyber Recommendations](#)
-

National Telecommunications and Information Administration Recommends Revoke China Telecom's Common Carrier Status

Introduced – April 2020

Summary

The NTIA said that its filing “represents agreement among the Departments of Justice, Homeland Security, Defense, State, Commerce, and the U.S. Trade Representative (USTR)” that allowing China Telecom to carry that voice traffic poses a “substantial and unacceptable national security and law enforcement risk associated with China Telecom’s continued access to U.S. telecommunications infrastructure. In the current environment, the national security and law enforcement risks cannot be mitigated.”

Reference Links

- [NTIA recommends revoking China Telecom’s common carrier status](#)
 - [China Telecom fights for US license](#)
 - [Trump administration moves to revoke China Telecom's US licenses on security grounds](#)
 - [DOJ Asks FCC to Ban China Telecom, Citing National Security](#)
-

FCC To Crack Down On Sharing Of Mobile Users’ Location Data

Introduced – February 2020

Summary

On January 31, 2020, Federal Communications Commission (FCC) Chairman Ajit Pai wrote in a letter to Congress that wireless networks that sold their customers’ real-time location data violated U.S. law. Pai said “a formal notice of liability” affecting at least one wireless firm would be sent by him to the five-member FCC commission. AT&T has already claimed that selling location data wasn’t illegal. If a common understanding is not reached, this could lead to imminent legal battles between the FCC and telecommunication companies.

Reference Links

- [FCC To Crack Down On Sharing Of Mobile Users’ Location Data](#)
 - [Ajit Pai: Carrier sales of phone-location data is illegal, FCC plans punishment](#)
 - [FCC confirms carriers ‘apparently’ broke the law by selling real-time customer locations](#)
-

Federal Trade Commission (FTC)

FTC Delivers Congressional Reports on Consumer Privacy Work

Introduced – March 2020

Summary

The Federal Trade Commission (FTC) has delivered two congressionally-requested reports on the agency's consumer privacy work as part of the fiscal year 2020 spending bill that funds FTC and other agencies.

The first report details the way FTC uses its authorities to protect consumer privacy and security and to "deter unfair and deceptive conduct." The report is in response to the Senate Appropriations Committee Report accompanying the FY2020 Financial Services and General Government Appropriations Bill.

The second report outlines how FTC utilizes resources for protecting consumer privacy and security. Additionally, it covers what further resources would be needed to expanded FTC efforts.

Reference Links

- [FTC Report on Resources Used and Needed for Protecting Consumer Privacy and Security](#)
 - [FTC's Use of Its Authorities to Protect Consumer Privacy and Security](#)
 - [FTC Delivers Reports on Consumer Privacy Work](#)
-

Government Accountability Office (GAO)

GAO Auditing Expanded Telework and Continuity of Operations Results

Introduced – June 2020

Summary

As part of the Coronavirus Aid, Relief and Economic Security (CARES) Act, the Government Accountability Office will oversee and audit how federal agencies are operating in their telework environments.

Reference Links

- [GAO to begin auditing response to expanded telework, continuity of operations](#)
 - [GAO plans review of telework tech](#)
-

General Services Administration (GSA)

GSA Issues Guidance to Improve Data Encryption on .gov Sites

Introduced – June 2020

Summary

GSA plans to get all websites with the .gov internet domain to use a standard that always encrypts a user's connection to that site. Additionally, by Sept. 1, 2020 the HTTP Strict Transport Security feature must be enabled automatically for all new federal websites that come online. Meeting the deadline will require cooperation between federal, state, local and tribal government bureaucracies.

Reference Links

- [Feds aim to bolster data encryption practices for .gov websites](#)
-

GSA 18F Project Investigates Factors that Contribute to Modernization Success

Introduced – June 2020

Summary

The General Services Administration's (GSA) 18F digital consulting arm has released a report aimed at identifying digital modernization approaches that will work on a long-term basis. The report, titled "The Best Practices in Digital Transformation", highlighted technical and infrastructure debts as major obstacles to iteration efforts in modernization programs. Some findings include:

- Government hierarchies also prevent teams from independently making decisions for transformation initiatives
- Direct feedback and diverse perspectives can help agencies establish cross-functional teams that produce actionable long-term results.

Reference Links

- [GSA Report Details Agencies' Obstacles to Digital Transformation](#)
 - [GSA 18F Project Investigates Factors that lead to Positive and Long-term Modernization Practices](#)
-

GSA Awards Funds to Secure 75 Micro Agencies

Introduced – May 2020

Summary

The General Services Administration, acting as the procurement arm for CDM, awarded CGI-Federal a \$276 million contract to provide 75 small and micro agencies — think Consumer Product Safety Commission or the Merit Systems Protection Board or the U.S. Institute of Peace — a host of services including a cyber catalog and a shared services platform.

Reference Links

- [75 small, micro agencies to have access to advanced cyber services under new award](#)
 - [DHS to standardize cyber protections through new contract](#)
 - [Continuous Diagnostics and Mitigation \(CDM\) Dynamic and Evolving Federal Enterprise Network Defense \(DEFEND\) Task Order \(TO\) Group F](#)
-

GSA Launches Beta Website for Federal Rulemaking Info

Introduced – May 2020

Summary

The General Services Administration (GSA) is working to update its web-based repository of information on government-issued documents and federal regulations as part of an initiative under the agency's eRulemaking program.

Reference Links

- [GSA Launches Beta Website for Federal Rulemaking Info](#)
-

GSA Unveils Database for Government-wide Contract Award Info

Introduced – May 2020

Summary

The General Services Administration (GSA) has launched a web-based tool in a move to consolidate information on the agency's government-wide contracting activities and visualize the allocation of contract obligations.

GSA said on the Government-Wide Category Management Reporting and Analytics website that the public database includes an awards exploration tool as well as a simplified interface for searching various information at the award level.

Reference Links

- [GSA Unveils Database for Governmentwide Contract Award Info](#)
 - [GSA releases tool for monitoring agency spending to contractors](#)
-

Controls Around the DotGov Program are Tightening Introduced – March 2020

Summary

GSA is enacting new requirements for validating the identity of people requesting them. The additional measures come less than four months after KrebsOnSecurity published research suggesting it was relatively easy for just about anyone to get their very own .gov domain. In order to increase public trust in .gov domains, GSA is now requiring a notarized letter as part of the application process.

Alternately in Congress, the DOTGOV Act of 2019, introduced by Sen. Gary Peters, D-MI, would transfer responsibility for .gov domains from the General Services Administration to the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency. It would also limit the fees the agency could charge to government agencies for registering .gov websites, establish grants to help jurisdictions move to .gov and create an outreach program to notify public officials about the program.

Reference Links

- [Now you need a notarized document to get a .gov domain](#)
 - [U.S. Govt. Makes it Harder to Get .Gov Domains](#)
 - [Bill Aims to Strengthen .Gov Program, Expand Municipal Use](#)
-

GSA Looks to Modernize Approach to Mitigating Fake Public Comments on Rulemakings

Introduced – February 2020

Summary

The General Services Administration has launched an effort to update its processes related to combating fake comments on federal rulemaking actions. GSA plans to modernize the procedures under its eRulemaking Program, which leverages shared services that enable the public to submit comments and review dockets through an electronic platform.

Reference Links

- [GSA Looks to Modernize Approach to Mitigating Fake Public Comments on Rulemakings](#)
 - [Before GSA can mitigate fake comments on rulemakings, it needs to know how prevalent they are](#)
-

GSA officials rethink ATO process, workforce reskilling to field AI tools faster

Introduced – February 2020

Summary

The General Services Administration and Federal Chief Information Officer Suzette Kent stood up a government-wide AI Community of Practice last November. Since then, membership has grown to more than 400 members from 26 agencies. The AI community of practice, said Steven Babitch, the head of GSA's AI portfolio, is looking at building a searchable "use case repository" that would give agencies a playbook of examples where agencies have successfully deployed AI for customer experience, human resources, advanced cybersecurity and business processes.

Members of the AI community of practice, he added, plan to hold quarterly meetings, but have also considered setting up webinars, seminars, workshops and other training to keep federal employees in the loop.

Reference Links

- [GSA officials rethink ATO process, workforce reskilling to field AI tools faster](#)
 - [What's in store for the GSA's AI community of practice?](#)
 - [Government developing AI use case repository for agencies facing challenges](#)
-

GSA, Labor Department Launch AI CoE Project

Introduced – February 2020

Summary

The General Services Administration (GSA) and the Department of Labor (DOL) are partnering on a new artificial intelligence (AI) Centers of Excellence (CoE) initiative. GSA's Technology Transformation Services (TTS) office will help DOL modernize its acquisition capabilities using

robotics process automation (RPA). While the project begins in the acquisition department, DOL hopes to scale the capability through the agency as a shared service.

Reference Links

- [GSA, Labor Department Launch AI CoE Project](#)
-

Department of Homeland Security (DHS)

CISA Released the First in its Cyber Essentials Toolkit Series

Introduced – June 2020

Summary

As a follow-up to the November 2019 release of Cyber Essentials, the Cybersecurity and Infrastructure Security Agency (CISA) released the first in a series of six Cyber Essentials Toolkits. This is a starting point for small businesses and government agencies to understand and address cybersecurity risk as they do other risks. CISA's toolkits will provide greater detail, insight and resources on each of the Cyber Essentials' six "Essential Elements" of a Culture of Cyber Readiness.

Reference Links

- [Cyber Essentials Toolkits](#)
 - [CISA Releases New Cyber Essentials Toolkit](#)
 - [ESSENTIAL ELEMENT: YOURSELF, THE LEADER](#)
 - [CISA Security Playbooks Get SMBs, Government Agencies Cyber Ready](#)
-

Congressional Letter and Internal Report Characterize CIA Cyber-security Controls as "Woefully Lax"

Introduced – June 2020

Summary

Sen. Ron Wyden (D-Ore.), released a letter that admonishes the CIA's Center for Cyber Intelligence (CCI) for failing to meet cybersecurity best practices for weaknesses that were present in their internal 2017 report on the Vault7 WikiLeaks disclosures. He characterizes the

“woefully lax” cyber posture as the result of a culture that “prioritized building cyber weapons at the expense of securing their own systems.”

Wyden recommended that Congress rescind any and all exceptions to the DHS cyber-security rules.

Reference Links

- [Report slams ‘woefully lax’ cyber-security controls at CIA](#)
 - [Widespread Cybersecurity Problems Across Intelligence Community, Claims US Senator Ron Wyden](#)
 - [Theft of CIA’s ‘Vault 7’ Secrets Tied to ‘Woefully Lax’ Security](#)
 - [CIA Report Slammed Agency’s Security as “Woefully Lax”](#)
-

GAO Calls on DHS to Improve Agile Metrics, Training, and Planning

Introduced – June 2020

Summary

The Government Accountability Office (GAO) has recently examined DHS’s adoption of Agile software development to assess the extent to which the department has addressed selected leading practices for its transition.

GAO recommended DHS fully implement leading practices for adopting Agile software development to improve the process of acquiring information technology systems. GAO found that DHS fully implemented the practice of planning for organizational change as part of its transition to Agile development, but partially executed the two practice areas – the need to implement and measure the impact of undertaking a significant change.

Of the 202 activities related to 18 Agile action plans, DHS completed 134 activities but pushed back approximately 34 percent of activities to a later date.

GAO offered 10 recommendations, such as establishing Agile training requirements for senior stakeholders, measuring results in relation to Agile adoption, developing a set of core performance metrics and creating new guidance on Agile methodologies.

Reference Links

- [GAO on Agile Software Development: DHS Makes Progress but Must Improve Metrics, Training and Planning](#)
 - [GAO: DHS Needs to Take Additional Steps in Transition to Agile Software Development](#)
-

CISA Releases Strategy to Improve ICS Cyber-Resiliency

Introduced – June 2020

Summary

The strategy seeks to promote the use of data analytics and technology platforms and advance training to help protect operators of transportation, energy and other critical infrastructure from foreign threat actors.

Reference Links

- [CISA Unveils Strategy to Protect Industrial Control Systems From Hackers; Christopher Krebs Quoted](#)
 - [DHS's cyber wing pledges to invest more in industrial control systems security](#)
-

DHS Warns of Security Issues in Devices from Baxter, BD and Biotronik

Introduced – June 2020

Summary

The Industrial Control Systems' Computer Emergency Response Team - a unit of Department of Homeland Security's Cybersecurity and Infrastructure Security Agency - issued six alerts about vulnerabilities in medical devices from Baxter, BD and Biotronik. Some of the flaws - if exploited - could result in compromises of patient information and allow attackers to alter data or system configurations or launch a distributed denial-of-service attack.

Reference Links

- [Alerts: Vulnerabilities in 6 Medical Devices](#)
-

GAO issues chemical facility protection recommendations

Introduced – May 2020

Summary

The Government Accountability Office (GAO) has issued the Department of Homeland Security (DHS) a series of recommendations regarding chemical facility cybersecurity oversight. DHS guidance designed to aid 3,300 facilities in complying with cybersecurity and other standards

has not been updated in over 10 years, and its cybersecurity training program for inspectors does not follow some essential training practices.

The GAO issued recommendations, including that the Assistant Director of the Infrastructure Security Division should implement a documented process for reviewing and, if necessary, revise its guidance for implementing cybersecurity measures at regularly defined intervals; and incorporate measures to assess the contribution that its cybersecurity training is making to program goals, such as inspector- or program-specific performance improvement goals. It was also recommended that DHS track delivery and performance data for its cybersecurity training, such as the completion of courses, webinars, and refresher training; develop a plan to evaluate the effectiveness of its cybersecurity training, such as collecting and analyzing course evaluation forms; develop a workforce plan that addresses the program's cybersecurity-related needs, which should include an analysis of any gaps in the program's capacity and capability to perform its cybersecurity-related functions, and human capital strategies to address them; and maintain reliable, readily available information about the cyber integration levels of covered chemical facilities and inspector cybersecurity expertise.

Reference Links

- [GAO: Chemical Plants Vulnerable to Cyberattacks](#)
 - [GAO issues chemical facility protection recommendations](#)
 - [GAO Tells CISA to Better Protect High-Risk Chemical Facilities from Cyber Attacks](#)
 - [Cybersecurity Guidelines for U.S. High-Risk Chemical Facilities Are a Decade Old](#)
-

FBI, CISA Warn of Chinese State-Backed Hackers Targeting COVID-19 Research Orgs Introduced – May 2020

Summary

The FBI and the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CIAS) have called on organizations conducting research related to COVID-19 to implement cybersecurity measures to protect their work from foreign threat actors.

Cyber actors with ties to the Chinese government have been observed targeting U.S. research organizations to gain access to public health data and intellectual property related to vaccines and testing.

Reference Links

- [The Healthcare Research Security Pandemic: Threats to Patient Care, National Security, and the Economy](#)
 - [FBI, CISA Warn of Chinese State-Backed Hackers Targeting COVID-19 Research Orgs](#)
 - [FBI, DHS Confirm China-Backed COVID-19 Hacking Activity](#)
-

DHS to Advise Telecom Firms 5G Infrastructure Security

Introduced – May 2020

Summary

The Department of Homeland Security is preparing to advise the U.S. telecom industry on steps it can take to prevent attacks on 5G cell towers following a rash of incidents in Western Europe fueled by the false claim that the technology spreads the pathogen causing covid-19.

The planned industry alert comes in the wake of dozens of arson attacks on 5G towers in Britain, the Netherlands and Belgium last month apparently spurred by the conspiracy theory.

Reference Links

- [US' DHS to advise telecom firms on how to prevent 5G cell tower attacks](#)
-

GAO: DHS Needs More Oversight for Service Contracts

Introduced – May 2020

Summary

The Homeland Security Department failed to create safeguards to prevent contracting out inherently governmental work, which could lead to loss of control over the department's mission, according to the Government Accountability Office. An appropriate balance of staff is needed to ensure contractors don't end up making policy in mission areas including cybersecurity.

Reference Links

- [GAO: DHS Needs More Oversight for Service Contracts](#)
-

DHS CISA and FBI share list of top 10 most exploited vulnerabilities

Introduced – May 2020

Summary

The Department of Homeland Security Cybersecurity and Infrastructure Security Agency (DHS CISA) and the Federal Bureau of Investigation (FBI) issued a report that urges organizations in the public and private sector to apply necessary updates in order to prevent the most common forms of attacks and exploited vulnerabilities. The list details the top 10 most commonly exploited software vulnerabilities across the last four years, between 2016 and 2019.

Reference Links

- [Top 10 Routinely Exploited Vulnerabilities](#)
 - [DHS CISA and FBI share list of top 10 most exploited vulnerabilities](#)
-

CISA Releases Supply Chain Security Resources

Introduced – May 2020

Summary

The Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) released the Information and Communications Technology (ICT) SCRM Essentials guide and the ICT SCRM Fact Sheet. The former will help agencies and organizations to start implementing SCRM, while the latter is an overview of ICT supply chain security and risk management.

Reference Links

- [CISA Establishes two Supply Chain Resources](#)
 - [ICT Supply Chain Risk Management Fact Sheet](#)
 - [ICT SUPPLY CHAIN RISK MANAGEMENT](#)
-

DHS, NCSC, and CISA Release Joint Advisory on COVID-19 Cyberthreats and Malicious Groups

Introduced – April 2020

Summary

The National Cyber Security Centre (NCSC), the U.S. Department of Homeland Security (DHS), and the Cybersecurity and Infrastructure Agency (CISA) have released a joint advisory describing the growing number of attackers and other malicious groups in the U.K. and the U.S.

These cybercriminals and advanced persistent threat (APT) groups are targeting individuals and organizations with a variety of ransomware and malware attacks or are otherwise exploiting the COVID-19 pandemic in their attack campaigns. The advisory also included a non-exhaustive list of indicators of compromise (IOCs) for cyberattacks detection and mitigation advice. It offers practical advice that individuals and organizations need to follow to mitigate the risk of being affected by cyberattacks. The IOCs provided within the accompanying .csv and .stix files of the advisory are based on analysis from CISA, NCSC, and other industry experts.

Reference Links

- [NCSC and CISA Release Joint Advisory on COVID-19 Cyberthreats and Malicious Groups](#)
 - [Advisory:COVID-19 exploited by malicious cyber actors](#)
-

CISA Releases Interim TIC 3.0 Guidance for COVID-19 Telework Surge

Introduced – April 2020

Summary

The Cybersecurity and Infrastructure Security Agency (CISA) released an interim Trusted Internet Connections (TIC) 3.0 guidance today focused on the rapid transition to telework as Federal agencies adjust their operations to combat spread of the COVID-19 coronavirus.

The TIC 3.0 Interim Telework Guidance supports Office of Management and Budget Memorandum 20-19, calling on agencies to “utilize technology to the greatest extent practicable to support mission continuity.” The document focuses on how remote Federal employees can securely connect to private government networks and cloud environments.

Reference Links

- [CISA Releases Interim TIC 3.0 Guidance for COVID-19 Telework Surge](#)
 - [TIC 3.0 Interim Telework Guidance](#)
-

DHS Categorizes DIB Personnel as “Essential” During the COVID-19 Crisis

Introduced – March 2020

Summary

Following the March 19, 2020 guidance issued by the Department of Homeland Security’s Cybersecurity and Infrastructure Agency (CISA) on “essential” critical infrastructure workers

during COVID-19, the Department of Defense (DoD) issued a memorandum today reiterating that the Defense Industrial Base (DIB) is identified as a critical infrastructure sector by DHS, and that those who work in such sectors are expected to maintain normal work schedules. The DHS guidance identified the DIB essential critical infrastructure workforce as those who provide “essential services to meet national security commitments,” including aerospace; mechanical and software engineers; manufacturing/production workers; IT support; security staff; security personnel; intelligence support; aircraft and weapon systems mechanics and maintainers; suppliers of medical supplies and pharmaceuticals; and critical transportation. The DoD memorandum adds some additional details, stating that DoD contracts and subcontracts that support the development, production, testing, fielding or sustainment of weapons systems/software systems or the manning, training, equipping, deploying, or support military forces, are considered essential critical infrastructure that should maintain normal work schedules.

Additionally, blockchain and agriculture organizations were also deemed essential.

Reference Links

- [DHS Issues Advisory “Memorandum on Identification of Essential Critical Infrastructure Workers During COVID-19 Response”](#)
 - [Department of Defense Issues Defense Industrial Base Memorandum](#)
 - [Homeland Security recognizes food, ag sectors as ‘essential](#)
 - [DHS Names Blockchain Managers Among Critical Infrastructure Workers](#)
-

CISA to act as Election Security Liaison Ahead of 2020

Introduced – March 2020

Summary

The Department of Homeland Security’s (DHS) Cybersecurity and Infrastructure Security Agency (CISA) is promising state and local election officials that it will be vigilant, trustworthy, and transparent about 2020 election security in the agency’s #Protect2020 Strategic Plan.

CISA officials hope to ramp up 2020 election security with efforts to continuously monitor threat trends, forecast vulnerabilities, safeguard the information of the American public, and quickly share cyber information with stakeholders.

Reference Links

- [#Protect2020](#)

- [CISA to act as Election Security Liaison Ahead of 2020](#)
-

CISA Releases Election Security Plan Following GAO Criticism

Introduced – February 2020

Summary

The Cybersecurity and Infrastructure Security Agency (CISA) released its #Protect2020 Strategic Plan for election security after the Government Accountability Office (GAO) criticized the agency's election security preparedness. The plan details CISA's four lines of election security effort – election infrastructure, campaign and political infrastructure, the American electorate, and warning and response – and key actions in each area. In its objectives, CISA has prioritized partnerships with the private sector, information sharing with stakeholders, and real-time cyber vulnerability assessments. Emergency response posters, interactive checklists, and infographics accompany the report as real-time tools that state and local election officials can use to inform and prepare their teams for 2020.

Reference Links

- [CISA Releases Election Security Plan Following GAO Criticism](#)
 - [CISA outlines its role in helping states with election security](#)
 - [#Protect2020](#)
 - [GAO report urges DHS to publish key security plans ahead of 2020 elections](#)
-

DHS Wants to Establish a New Internal Cyber Coordination Group

Introduced – February 2020

Summary

The Department of Homeland Security wants to establish an internal organization dedicated to coordinating cybersecurity efforts across DHS and identifying joint priorities. In its fiscal 2021 budget request, DHS asked Congress to allocate it \$2.6 million to create the Joint Cyber Coordination Group. The group would have six full-time employees and be housed under the Office of Policy, Strategy and Plans (PLCY). DHS' congressional justification say that it needs the group because expanding technological and cyber threats make it difficult for any one component to manage "all aspects of associated risk."

Reference Links

- [Homeland Security wants a new cyber coordination group](#)
-

DHS CyberOps Center Moving to IT Ops Directorate

Introduced – February 2020

Summary

The Cybersecurity Operations Center is moving from the CISO Directorate to the Information Technology Operations Directorate (ITO). The move will allow the CISO to focus on enterprise policy, compliance, and assessments in support of the DHS mission, including the expansion of the Cybersecurity Service Provider Program to include assessments of network operations centers.

Consolidating the security and network functions under ITO will increase collaboration and network integration, and a more integrated workflow under a single directorate will make it easier to deploy, implement, and respond to capabilities preventing intrusions.

Reference Links

[DHS CyberOps Center Moving to IT Ops Directorate](#)

Department of Justice (DOJ)

Revised DOJ Guidance Offers Tightens Risk-management Language

Introduced – June 2020

Summary

On June 1, 2020 the DOJ issued an update to its compliance guidance for prosecutors of white-collar crime to use when assessing whether a company complied with its own risk management program. The revision included new language to make sure compliance programs aren't merely one-and-done snapshots, but are instead dynamic programs that get updated to fit changing circumstances. The new guidance also asks prosecutors to make sure compliance programs are adequately resourced within organizations.

Prosecutors use this guidance to assess criminal liability in a compliance breach, so it behooves business and security leaders to understand the expectations.

Reference Links

- [Revised DOJ compliance guidance offers risk-management lessons for cybersecurity leaders](#)
-

DOJ Disrupts Hundreds of COVID-19 Scammer Domains

Introduced – April 2020

Summary

The Department of Justice announced April 22 that it has taken action to disrupt "hundreds" of internet domains that the government claims were participating in coronavirus-related scams to defraud Americans.

According to the announcement, the FBI's Internet Crime Complaint Center has received more than 3,600 complaints about websites peddling fake vaccines or cures, soliciting donations for fake charities, falsely representing themselves as public health organizations or exploiting concern over the virus to trick users into downloading malware.

Reference Links

- [Feds disrupt hundreds of COVID-19 scammer domains](#)
- [Hundreds of Online Virus Scams Shut Down by Justice Department](#)

- [DOJ thwarts hundreds of websites tied to coronavirus scams, security threats](#)
-

DOJ Launches Coronavirus Cybercrime Task Force

Introduced – March 2020

Summary

The U.S. Justice Department and the Commonwealth of Virginia announced the creation of a special task force dedicated to stamping out fraudulent activities that seek to profit off the growing pandemic caused by the novel coronavirus, including online scams that steal money from victims or install malware.

Reference Links

- [Coronavirus cybercrime task force launches in Virginia](#)
-

DOJ Charges Four Chinese Military Officers in Equifax Breach

Introduced – February 2020

Summary

The US Justice Department has held four members of China's People's Liberation Army (PLA) responsible for the Equifax data breach. A federal grand jury in Atlanta charged the PLA members for stealing Equifax's "valuable trade secrets" and personal data of its customers.

The announcement read, "The nine-count indictment alleges that Wu Zhiyong, Wang Qian, Xu Ke and Liu Lei were members of the PLA's 54th Research Institute, a component of the Chinese military. They allegedly conspired with each other to hack into Equifax's computer networks, maintain unauthorised access to those computers, and steal sensitive, personally identifiable information of approximately 145 million American victims."

Reference Links

- [Equifax hack: USA charges four Chinese military officers](#)
 - [DOJ Charges Against Chinese Concerns Alert US Businesses To Watch Their Supply Chains](#)
-

DOJ Charges Huawei with Racketeering, Illegal Trade with Iran and North Korea

Introduced – February 2020

Summary

The On February 13, 2020, the United States Department of Justice announced charges against Huawei Technologies Co. Ltd. for conspiracy to violate the Racketeer Influenced and Corrupt Organizations Act, also known as RICO. The charges were contained in a superseding indictment, which has 16 counts in addition to a charge of conspiracy to steal trade secrets.

According to the charges, Huawei successfully stole intellectual property from six unnamed American technology companies. That intellectual property reportedly includes proprietary information involving robotics, cell phone antennas, and source code for internet routers.

The Justice Department says Huawei stole much of the information by simply violating confidentiality agreements with companies whose information they stole. Other information was allegedly stolen through intermediaries, including professors at research institutes or former employees of rival tech companies, whom Huawei asked to provide classified information. Huawei even had a policy in place to reward employees who obtained valuable information.

The FBI also claims that a Huawei subsidiary engaged in forbidden trade with countries under sanction, including Iran and North Korea.

Reference Links

- [DoJ Charges Huawei with Racketeering, Illegal Trade with Iran and North Korea](#)
 - [US charges Huawei with racketeering and conspiracy to steal trade secrets](#)
-

Department of Health and Human Services (HHS)

HHS Suffers Cyber Incident, Remains Fully Operational

Introduced – March 2020

Summary

In the midst of the coronavirus outbreak, HHS was the victim of a DDoS attack. The intent of the attack was to slow systems, though it was largely unsuccessful, no data was compromised and HHS remained "fully operational."

The attack may have been the result of "multiple incidents of hacking." While the perpetrator hasn't been identified, officials believe it was orchestrated by nation-state actors. The attack may have been preempted by a campaign spread by text, email, and social media, warning that President Donald Trump intended to order a mandatory two-week quarantine across the country. The National Security Council warned about these fake messages, calling them rumors and urging all to listen to guidance from the Centers for Disease Control and Prevention.

Despite HHS assurances that layered security controls are implemented, Sen. Michael Bennet (D-Colo.) has pushed for a review of "all computer-based IT and network systems at the Department of Health and Human Services (HHS), Centers for Disease Control and Prevention (CDC), and the National Institute of Health."

Reference Links

- [HHS hit with cyberattack as US deals with coronavirus response](#)
 - [As HHS Responds to Coronavirus, Network Targeted by Cyberattack](#)
 - [HHS saw increase in network scanning in midst of COVID-19 outreach](#)
 - [HHS chief refutes cyberattack, says added security is in place](#)
 - [US health agency suffers cyberattack amid COVID-19 outbreak](#)
 - [Senator Pushes For HHS Cybersecurity Measures After Incident](#)
-

National Institute of Standards and Technology (NIST)

NIST Releases Guidance for IoT Device Manufacturers

Introduced – June 2020

Summary

NISTIR 8259 “Foundational Cybersecurity Activities for IoT Device Manufacturers” provides six activities that IoT manufacturers can use to inform primarily the manufacturing of new devices:

- Identify expected customers and users, and define expected use cases.
- Research customer cybersecurity needs and goals.
- Determine how to address customer needs and goals.
- Plan for adequate support of customer needs and goals.
- Define approaches for communicating to customers.
- Decide what to communicate to customers and how to communicate it.

The suggested activities emphasize understanding the customer, including how the customer will interact with the device, how the customer can be informed of security features, and device security lifecycle considerations. Beyond technical measures, such as software, the customer is an integral piece of the proposed security solution – without customer understanding, advanced features and technical countermeasures may not be of much use.

NISTIR 8259A “IoT Device Cybersecurity Capability Core Baseline” provides six baseline device cybersecurity capabilities. These baseline elements are meant to be extensible and solution agnostic in order to provide implementation flexibility. Device manufacturers would do well to review the provided rationales in light of described cybersecurity capability to inform ultimate implementation decisions. The six provided device cybersecurity capabilities are:

- Device Identification
- Device Configuration
- Device Protection
- Logical Access to Interfaces
- Software Update
- Cybersecurity State Awareness

Reference Links

- [NISTIR 8259: Foundational Cybersecurity Activities for IoT Device Manufacturers](#)
- [NISTIR 8259A: IoT Device Cybersecurity Capability Core Baseline](#)

- [NIST Provides Important Guidance For IOT Industry](#)
- [NIST Releases Cybersecurity Guidance for Manufacturers of IoT Devices](#)

NIST Opens Applications for Digital Forensics Exercise

Introduced – June 2020

Summary

NIST is looking for public and private sector experts to take part in an exercise focused on evaluating the digital forensics community's capacity to conduct mobile- and computer-based investigations.

NIST said the three-month online exercise will deploy a "black box" concept to assess the performance of digital capabilities in processing simulated evidence for real-life cases including homicide and intellectual property theft. Participants will undergo a two-hour exam and download the digital evidence from NIST's website. Forensic resources must be processed through one virtual computer and one mobile phone. According to NIST, participants will be allowed to use "whatever forensic software tools they choose" to answer questions during the test which is aimed at evaluating the reliability of experts' methods for producing results.

Reference Links

- [NIST to Digital Forensics Experts: Show Us What You Got](#)
 - [NIST Opens Applications for Digital Forensics Exercise](#)
-

NIST Releases Final Version of SP 1800-23 Guides Identification of Threats to OT Assets

Introduced – June 2020

Summary

In late May, the NCCoE released the final version of NIST SP 1800-23. NIST SP 1800-23 is a response to the growing digital security challenges confronting organizations with operational technology (OT) assets.

Reference Links

- [SP 1800-23, Energy Sector Asset Management.](#)
 - [Final Version of NIST SP 1800-23 Guides Identification of Threats to OT Assets](#)
 - [Final Version of NIST SP 1800-23 Guides Identification of Threats to OT Assets](#)
-

NIST Requests Feedback on Digital Identity and Biometric Guidelines

Introduced – June 2020

Summary

The National Institute of Standards and Technology has issued a call for comments on its digital identity guidelines contained in four documents.

The agency is seeking review and feedback on its:

- SP 800-63-3 Digital Identity Guidelines
- SP 800-63A Enrollment and Identity Proofing
- SP 800-63B Authentication and Lifecycle Management
- SP 800-63C Federation and Assertions

which collectively provide the controls and technical requirements for specified digital identity management assurance levels.

The review is needed because of a policy memo from the Office of Management and Budget (OMB) directing federal agencies to boost their identity and access management capabilities and asking NIST to update its guidance, as well as changes to the NIST Cybersecurity Framework and Privacy Framework, and the OMB policy memoranda on COVID-19 response and mission continuity.

Comments are due by August 10, 2020.

Reference Links

- [PRE-DRAFT Call for Comments: Digital Identity Guidelines](#)
 - [NIST requests feedback on digital identity guidelines, including for behavioral biometrics and liveness](#)
-

NCCoE Designates 10 Tech Partners in Industrial Control System Security Initiative

Introduced – March 2020

Summary

The NCCoE has asked 10 vendors to develop an approach for the manufacturing sector to protect integrity of data in industrial control systems. Collaborators agreed to provide hardware or software and services to help NCCoE create a reference and implement example standards for industry.

The consortium aims to produce a guide that will outline practical methods to comply with cybersecurity standards from NIST and the private sector. The project collaborators are:

- CyberX
- Dispel
- Dragos
- GreenTec USA
- ForeScout Technologies
- OSIsoft
- Radiflow
- Tenable
- TDi Technologies
- VMware

Reference Links

- [NIST Center Names 10 Tech Industry Participants in Industrial Control System Security Initiative](#)
 - [New Tech Companies Sign on to NCCoE ICS Security Project](#)
 - [NCCoE announces 10 technology collaborators for Protecting Information and System Integrity in Industrial Control System Environments project](#)
-

NIST Issues IAST and RASP Guidance

Introduced – March 2020

Summary

NIST released a revision to Security and Privacy Controls for Information Systems and Organizations, NIST SP 800-53 Revision 5. Those responsible for application security need to capitalize on two new standards that address interactive application security testing (IAST) and

runtime application self-protection (RASP). The following synopsis from each standard best summarizes the requirements:

- SA-11(9): “Require the developer of the system, system component, or system service to employ interactive application security testing tools to identify flaws and document the results.”
- SI-7(17): “Implement [Assignment: organization-defined controls] for application self-protection at runtime.”

Reference Links

- [New NIST Standards on IAST and RASP Deliver State-of-the-Art AppSec](#)
-

NIST Announces Workshop Focused on "Bias in AI"

Introduced – March 2020

Summary

NIST announced a workshop focused on understanding and addressing bias in Artificial Intelligence (AI) systems. The event will bring together members of the public and private sector to seek consensus on what 'bias' means in the context of AI and how to measure it.

The workshop will be held virtually on August 18, 2020, and organizations looking to take concrete actions to reduce biases based on race, ethnicity, gender, sexuality, and other protected characteristics in their products should consider participating.

Reference Links

- [Bias in AI Workshop](#)
 - [NIST Announces Workshop Focused on "Bias in AI"](#)
-

NIST Releases Update for Draft FedRAMP Controls Baseline Guide

Introduced – March 2020

Summary

(NIST) has issued an updated version of its Open Security Controls Assessment Language (OSCAL) milestone that includes guidelines for control baselines and system security plans (SSP) for various hardware and software.

NIST explained the OSCAL Milestone 3 serves as an official prerelease of the full OSCAL v1 and includes additional draft models for machine-readable formats such as XML, JSON and YAML.

OSCAL serves as a collaborative effort between NIST and Federal Risk and Authorization Management Program (FedRAMP) intended to help speed up the latter's authorization process.

According to NIST, the OSCAL team will continue collecting feedback on Milestone 3 to inform the development of more tutorials, layers and models. The agency added that it also seeks developers and offerors to support OSCAL implementation for commercial as well as open-source applications.

OSCAL Milestone 3's release comes after FedRAMP issued its OSCAL SSP Template and Guidance.

Reference Links

- [OSCAL 1.0.0 Milestone 3 Release](#)
 - [NIST Releases Update for Draft FedRAMP Controls Baseline Guide](#)
-

NIST Invites Industry to Demonstrate 5G-Security Platforms Introduced – May 2020

Summary

The National Institutes of Standards and Technology's (NIST) National Cybersecurity Center of Excellence (NCCoE) is asking industry to demonstrate products and technical expertise to support its project entitled, 5G Cybersecurity: Preparing a Secure Evolution. According to the notice, "NIST is soliciting responses from all sources of relevant security capabilities to enter into a Cooperative Research and Development Agreement (CRADA) to provide products and technical expertise to support and demonstrate security platforms for the 5G Cybersecurity: Preparing a Secure Evolution to 5G project."

The project will attempt to demonstrate how 5G architecture components can provide security capabilities that can mitigate risks and meet industry sectors' compliance requirements. It will ultimately result in a NIST Practice Guide as a Special Publication 1800 series that will be publicly available.

Reference Links

- [NIST Invites Industry to Demonstrate 5G-Security Platforms](#)
- [NIST Wants Orgs to Contribute Products to Support 5G Cybersecurity Demo Project](#)

- [NIST Wants Help Demonstrating Security Compliance in 5G](#)
-

NIST Introduces Framework for Secure Software Development

Introduced – May 2020

Summary

NIST Cybersecurity recently published a whitepaper outlining software development practices, known collectively as a secure software development framework (SSDF), that can be implemented into the software development lifecycle (SDLC) to better secure applications. The outlined practices are based on pre-established standards and guidelines as well as software development practice documents.

Reference Links

- [Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework \(SSDF\)](#)
 - [NIST Introduces Framework for Secure Software Development](#)
-

NIST Offers Guidance on Evaluating Information Security Monitoring Programs

Introduced – May 2020

Summary

The National Institute of Standards and Technology (NIST) released guidance on how to assess Information Security Continuous Monitoring (ISCM) programs for commercial entities as well as Federal, state, and local government organizations. The guidance, NIST Special Publication 800-137A, “can be used as presented or as the starting point for an organization-specific methodology,”

Reference Links

- [NIST Offers Guidance on Evaluating Information Security Monitoring Programs](#)
 - [NIST Special Publication 800-137A: Assessing Information Security Continuous Monitoring \(ISCM\) Programs](#)
-

NIST Shares Cyber Risk Management, Mobile Guides; Impact Analysis Tool

Introduced – April 2020

Summary

NIST released several updates and draft frameworks around enterprise risk management and cybersecurity, and mobile device security for comment, as well as a supply chain impact analysis tool.

The draft Integrating Cybersecurity and Enterprise Risk Management guidance addresses a wide range of risks. It seeks to promote a greater understanding of the relationship between cybersecurity risk management and overall risk, as well as the benefits of integrating the processes. Organizations can leverage the framework to improve cybersecurity risk information, provided as inputs to an overall risk management process.

NIST is also working to update its flagship guidance for Security and Privacy Controls for Information Systems and Organizations for the first time in seven years. The framework sheds light on a range of devices from IoT to general-purpose computers.

NIST also recently released draft guidance for Managing the Security of Mobile Devices in the Enterprise, designed to help organizations manage mobile device security threats. The publication outlines technologies and strategies for mitigating these threats, as well as recommendations for secure deployment, use, and disposal of mobile devices.

Lastly, NIST released a prototype impact analysis tool for interdependent cyber supply chain risks, designed to fill the gap between an organization's "risk appetite" and supply chain risk posture. IT provides a basic measurement of the potential impact of a cyber supply chain event.

Reference Links

- [Integrating Cybersecurity and Enterprise Risk Management \(ERM\)](#)
 - [NIST Updates and Expands Its Flagship Catalog of Information System Safeguards](#)
 - [Guidelines for Managing the Security of Mobile Devices in the Enterprise](#)
 - [NIST Shares Cyber Risk Management, Mobile Guides; Impact Analysis Tool](#)
-

NCCoE Soliciting Feedback on “Methodology for Characterizing Network Behavior of Internet of Things” White Paper

Introduced – April 2020

Summary

The National Cybersecurity Center of Excellence (NCCoE) is requesting feedback until May 1, 2020 on a Draft NIST Cybersecurity White Paper, Methodology for Characterizing Network Behavior of Internet of Things Devices. It demonstrates how to use device characterization

techniques to describe the communication requirements of Internet of Things (IoT) devices in support of the NCCoE's manufacturer usage description (MUD) project.

Reference Links

- [Draft NIST White Paper on “Methodology for Characterizing Network Behavior of Internet of Things](#)
 - [Methodology for Characterizing Network Behavior of Internet of Things Devices](#)
-

NIST Considers DevSecOps Framework for Agencies

Introduced – April 2020

Summary

The National Institute of Standards and Technology is considering creating a DevSecOps framework for agencies to make embedding security controls at the beginning of the software development lifecycle a common practice. NIST is “currently gathering information on products developed using DevSecOps” to be “distilled into NIST guidance that, while offering a clear perspective, will be designed to let agencies innovate on DevSecOps implementations.

Reference Links

- [NIST Considers DevSecOps Framework for Agencies](#)
 - [NIST exploring possible DevSecOps framework for agencies](#)
-

NICE Providing Online Cybersecurity Training Resources

Introduced – April 2020

Summary

Under the National Initiative for Cybersecurity Education (NICE), the National Institute of Standards and Technology (NIST) has provided links to free and low-cost online cybersecurity educational content.

NIST also added that some of the online resources may contribute towards professional learning objectives or lead to certifications and online degrees. The list will continue to be updated and already includes courses from local community colleges, four-year universities, and the Centers of Academic Excellence programs.

Some of the programs available on the webpage include:

- Pluralsight video courses;
- Chief Information Security Officer Workshop Training;
- Fundamentals of Cybersecurity Information for middle and high school students; and
- NIST Cybersecurity Professional Awareness Training.

Reference Links

- [NIST Providing Online Cybersecurity Training Resources](#)
-

NIST Seeking Public Comments on Integrating Cybersecurity and Enterprise Risk Management (ERM) Framework

Introduced – March 2020

Summary

The National Institute of Standards and Technology is asking for public comments on a new report that provides insight into how organizations can integrate cybersecurity into enterprise risk management.

The document, titled “NIST-Interagency Report 8286 Integrating Cybersecurity and Enterprise Risk Management,” advises organizations on how to improve the cybersecurity risk information they use to shape their enterprise risk management program.

The report suggests that communications about cybersecurity risk need be had between systems’ cybersecurity professionals, organizations’ high-level executives and the enterprises’ corporate leaders. By doing so, NIST wrote that the enterprise and system owners will all have a better idea of how to identify, assess and manage cybersecurity risk in relation to business missions.

Reference Links

- [Draft NISTIR 82861 Integrating Cybersecurity and 2 Enterprise Risk Management \(ERM\)](#)
 - [NIST asks for public comments on new cybersecurity risk management document](#)
-

NST Offers Telework Security Guidance

Introduced – March 2020

Summary

NIST released a bulletin note from the Information Technology Laboratory (ITL) on cybersecurity risks increasing with remotely accessible telework networks. ITL says that agencies and organizations should assume that malicious cyber actors will try to gain access to agency systems and that they'll try to leverage telework devices to gain access to the enterprise network or attempt to recover sensitive data. ITL states that organizations should assume that communications on external networks are susceptible to eavesdropping, interception, and modification.

The ITL bulletin summarizes recommendations from NIST Special Publication 800-46 Revision 2, Guide to Enterprise Telework, Remote Access, and Bring Your Own Device Security, including:

- “Developing and enforcing a telework security policy, such as having tiered levels of remote access;
- [Requiring] multi-factor authentication for enterprise access;
- Using validated encryption technologies to protect communications and data stored on the client devices;
- Ensuring that remote access servers are secured effectively and kept fully patched; and
- Securing all types of telework client devices against common threats.”

Additionally, the bulletin includes information on different types of remote access working and highlights what kind of security concerns can be involved.

Reference Links

- [NIST offers tips for secure telework](#)
 - [NIST Special Publication 800-46Revision: Guide to Enterprise Telework, Remote Access, and Bring Your Own Device \(BYOD\) Security](#)
 - [NIST: Assume Telework Networks Will be Compromised](#)
-

NIST Releases Roadmap on How to Build Cybersecurity Workforce

Introduced – March 2020

Summary

NIST released a report outlining best practices in building the cybersecurity workforce through regional partnerships. The National Initiative for Cybersecurity Education (NICE) is addressing the critical issue by energizing and promoting a robust network and ecosystem of cybersecurity education, training, and workforce development. Supporting this mission, objective 3.3 of the NICE Strategic Plan emphasizes guiding career development and workforce planning by

facilitating state and regional consortia to identify cybersecurity pathways addressing local workforce needs.

NIST says that by fostering regional alliances:

- workforce needs of local business and non-profit organizations are better aligned with the learning objectives of education and training providers conforming to the NICE Cybersecurity Workforce Framework,
- the pipeline of students pursuing cybersecurity careers is enlarged,
- more Americans are upskilled and moved into middle-class jobs in cybersecurity, and
- local economic development to stimulate job growth is supported.

Reference Links

- [NIST Releases Roadmap on How to Build Cybersecurity Workforce](#)
 - [NISTIR 8287 A Roadmap for Successful Regional Alliances and Multistakeholder Partnerships to Build the Cybersecurity Workforce](#)
 - [NIST Shares Workforce Development, Cybersecurity Partnership Insights](#)
 - [NIST puts forward regional roadmap to fill the cyber skills gap](#)
-

NIST Releases Tool to Measure the Impact of Supply Chain Risk Introduced – March 2020

Summary

The National Institute of Standards and Technology (NIST) has developed a prototype tool developed to show a possible solution for filling the gap between an organization's risk appetite and supply chain risk posture by providing a basic measurement of the potential impact of a cyber supply chain event.

While the Cyber Supply Chain Risk Management (C-SCRM) Interdependency Tool does not represent a complete supply chain risk management solution, it can be integrated into or used in concert with tools such as third-party management, enterprise resource planning, and supply chain management efforts.

The tool also provides the user with greater visibility over the supply chain and the relative importance of particular projects, products, and suppliers (which NIST refers to as "nodes") compared to others. This can be determined by examining the metrics which contribute to a node's importance, such as the amount of access a node has to the acquiring organization's IT network, physical facilities, and data.

NIST is seeking comments related to additional functionality or other aspects of the tool which may be used to develop future versions of the software. Comments should be addressed to scrm-nist@nist.gov by April 17, 2020.

Reference Links

- [NIST Seeks to Mitigate Supply Chain Risk, as COVID-19 Impacts Industry](#)
- [Draft NISTIR 8272: Impact Analysis Tool for Interdependent 3 Cyber Supply Chain Risks](#)

NIST Releases Draft Guidance on Supply Chain Security

Introduced – February 2020

Summary

The National Institute of Standards and Technology (NIST) has published a draft guidebook for businesses that presents a set of effective risk management techniques distilled by NIST's computer security experts.

"Key Practices in Cyber Supply Chain Risk Management" provides a set of strategies to help businesses address the cybersecurity issues posed by modern information and communications technology products, which are commonly built using components and services supplied by third-party organizations. The composed nature of these devices and systems makes them difficult to secure effectively against malware and other threats, placing manufacturers, service providers, and end users at risk.

Reference Links

- [Key Practices in Cyber Supply Chain Risk Management: Observations from Industry](#)
 - [NIST releases draft guidebook for addressing supply chain cybersecurity](#)
 - [NIST releases publication on how businesses can minimize cybersecurity risk](#)
 - [NIST offers providers tips for protecting complex cyber supply chains](#)
 - [NIST Releases Draft Guidance on Supply Chain Security](#)
 - [NIST Shares Cyber Supply Chain Risk Management Guidance](#)
 - [NIST Releases Cyber Supply Chain Draft Guidance](#)
-

NIST seeks comment on ransomware and cyberattack guidance

Introduced – February 2020

Summary

NIST's National Cybersecurity Center of Excellence (NCCoE) is seeking input on Special Publication 1800-25, which addresses "Identifying and Protecting Assets Against Ransomware and Other Destructive Events," and Special Publication 1800-26, which addresses "Detecting and Responding to Ransomware and Other Destructive Events." The NCCoE said the draft guides are intended to "benefit executives, chief information security officers, system administrators, or those who have a stake in protecting their organizations' data, privacy, and overall operational security." Both guides consist of three sections: an executive summary; a section on approach, architecture, and security characteristics; and how-to guides. They also both closely align with NIST Cybersecurity Framework version 1.1, published in April 2018.

Reference Links

- [NIST SPECIAL PUBLICATION 1800-25: Data Integrity - Identifying and Protecting Assets Against Ransomware and Other Destructive Events](#)
 - [NIST SPECIAL PUBLICATION 1800-26: Data Integrity - Detecting and Responding to Ransomware and Other Destructive Events](#)
 - [NIST seeks comment on ransomware, cyber-attack guidance](#)
 - [NIST Drafts Guidelines for Coping With Ransomware](#)
-

NIST Seeks Industry Support for Data Confidentiality Program

Introduced – February 2020

Summary

NIST has launched two data confidentiality projects and is calling on industry to "provide products and technical expertise to support and demonstrate security platforms." According to a Federal Register notice, NIST's National Cybersecurity Center of Excellence seeks partnerships to "establish tools and procedures to defend, detect, and respond to data confidentiality events" as part of the Data Confidentiality Building Block initiative.

The first effort will focus on identifying and protecting assets and data against breaches while the second project revolves around data breach detection, response and recovery activities.

The agency plans to issue a cybersecurity guide upon the completion of both projects. The building block effort is slated to begin no sooner than March 5.

Reference Links

- [National Cybersecurity Center of Excellence \(NCCoE\) Data Confidentiality Building Block](#)
- [NIST Seeks Industry Support for Data Confidentiality Program](#)
- [How NIST is exploring new data security best practices](#)

- [NCCoE Invites Letters of Interest for Data Confidentiality Projects](#)
-

SAMPLE

Office of Management and Budget (OMB)

Auditors Call on OMB to Ensure Agencies Coordinate on State Cybersecurity Requirements

Introduced – June 2020

Summary

According to GAO, The Office of Management and Budget can relieve some of the burden states face in complying with laws to manage the protection of federal information they access by enforcing the Federal Information Security Modernization Act (FISMA) of 2014, that compels federal agencies sharing personally identifiable information and other sensitive data with states must oversee the cybersecurity of those states' systems. State officials warn that duplicative and fragmented requests are sapping their resources.

Reference Links

- [Selected Federal Agencies Need to Coordinate on Requirements and Assessments of States](#)
 - [Auditors Call on OMB to Ensure Agencies Coordinate on State Cybersecurity Requirements](#)
 - [GAO: Federal Agencies Need to Coordinate on Requirements and Assessments of States](#)
 - [GAO Backs States in Call for Agency Cybersecurity Reforms](#)
-

OMB Is Clarifying Contracting Language and Security Liability in Cloud SLAs

Introduced – May 2020

Summary

COVID-19 sped up some agencies' cloud migration and amplified calls for cybersecurity assurances. As a result, the Office of Management and Budget plans to standardize language in all government contracts with cloud vendors that would update liability terms regarding security

Reference Links

- [The White House Is Rewriting Contracting Language to Clarify Security Liability](#)
 - [OMB Seeks to Clarify Security Liability in Cloud Contracts](#)
-

CISA Selected as Cybersecurity QSMO

Introduced – April 2020

Summary

The Office of Management and Budget (OMB) has selected the Cybersecurity and Infrastructure Security Agency (CISA) as the first formally designated Quality Service Management Office (QSMO) for cybersecurity services. Within the cybersecurity services division, CISA will act as QSMO for security operation center standardization, vulnerability management standardization, and domain name system resolver.

The QSMO initiative, issued in April 2019 as a part of Memorandum 19-16, creates centralized mission-support capabilities to promote the use of shared services.

Reference Links

- [CISA Selected as QSMO for Cybersecurity](#)
 - [CISA cleared to share cybersecurity services as first official QSMO](#)
 - [OMB Formally Designates CISA As Fed Lead For Shared Cyber Security Solutions](#)
-

OMB Requests \$45.8B Emergency Funds to Support Telework and Cybersecurity

Introduced – March 2020

Summary

The Office of Management and Budget (OMB) is requesting \$45.8 billion in Fiscal Year 2020 emergency funds to support the government-wide response to the COVID-19 coronavirus outbreak, including updates to agency IT to support telework and improve cybersecurity.

Reference Links

- [OMB Requests \\$45.8B Emergency Funds to Support Telework, Cyber](#)
-

OMB Updates Contracting and Technology Guidance for Federal Agencies

Introduced – March 2020

Summary

Following White House instructions to offer “maximum telework flexibilities” for federal employees, the Office of Management and Budget updated its agency guidance regarding millions of federal contractors.

The guidance, from OMB’s Deputy Director for Management Margaret Weichert, instructs agencies to do three main things:

1. Agencies are urged to work with their contractors, if they haven't already, to evaluate and maximize telework for contractor employees, wherever possible.
2. Agencies should be flexible in providing extensions to performance dates if telework or other flexible work solutions, such as virtual work environments, are not possible, or if a contractor is unable to perform in a timely manner due to quarantining, social distancing, or other COVID-19 related interruptions. Agencies should take into consideration whether it is beneficial to keep skilled professionals or key personnel in a mobile-ready state for activities the agency deems critical to national security or other high priorities. Additionally, agencies should also consider whether contracts that possess capabilities for addressing impending requirements such as security, logistics, or other function, may be retooled for pandemic response consistent with the scope of the contract.
3. Finally, agencies are encouraged to leverage the special emergency procurement authorities authorized in connection with the President's emergency declaration under section 501(b) of the Robert T. Stafford Disaster Relief and Emergency Assistance Act, 42 U.S.C. §§ 5121-5207 (the "Stafford Act"). These flexibilities include increases to the micro-purchase threshold, the simplified acquisition threshold, and the threshold for using simplified procedures for certain commercial items, all of which are designed to reduce friction for contractors, especially small businesses, and the government and enable more rapid response to the many pressing demands agencies face.

The contractor guidance follows calls from lawmakers and trade groups to address one of the largest components of the government’s workforce. The updated guidance also includes a frequently asked questions section addressing more nuanced questions for managers, including how to address contractor or employee exposure to COVID-19.

Reference Links

- [OMB Requests \\$45.8B Emergency Funds to Support Telework, Cyber](#)
-

Office of Personnel Management (OPM)

37 IGs Report on Agency Tech Challenges Related to \$2.4 Trillion COVID Relief Package

Introduced – June 2020

Summary

The Coronavirus Aid, Relief and Economic Security, or CARES, Act approved spending \$2.4 trillion to help the nation through the COVID-19 pandemic, almost all of which was disbursed through federal programs, or used directly to support agency operations. The Council of Inspectors General on Integrity and Efficiency—made up of inspectors general from across government—released an initial report identifying unique and common challenges agencies have faced managing the funds. IGs from 37 agencies contributed to the final report from the Pandemic Response Accountability Committee, which broke the common challenges into four “key areas of concern,” including IT security and management. These concerns are impacted by (1) widespread reliance on maximum telework to continue agency operations during the pandemic, which has strained agency networks and shifted IT resources, and (2) additional opportunities and targets for cyberattacks created by remote access to networks and increases in online financial activity.

Reference Links

- [37 IGs Report on Agency Tech Challenges Related to \\$2.4 Trillion COVID Relief Package](#)

OPM Report Highlights Human Capital Management Concerns in Federal Agencies

Introduced – April 2020

Summary

The Office of Personnel Management (OPM) issued a human capital review (HCR) report covering 2019 that emphasized hiring and retention obstacles for employees in STEM fields, and how to strategically develop the workforce and close the skills gap. Identified trends in federal agencies included:

- Administering compensation and benefits that lack flexibility;
- Identifying and closing skills gaps;
- Providing continuous learning and employee development;
- Recruiting and retaining employees;
- Adopting shared services and advanced systems;

- Implementing effective performance management systems;
- Adopting robotic process automation (RPA) and AI;
- Advancing human capital data analytics; and
- Achieving a strategic human capital management evaluation system.

Reference Links

[Agencies Identify Human Capital Management Concerns in OPM Report](#)

OPM Overhauls Cyber Talent Assessment

Introduced – March 2020

Summary

To address a critical need for cybersecurity personnel in the federal workforce, the Office of Personnel Management is overhauling its aptitude tests and other assessments used in recruiting needed IT talent.

In a memo issued to agency heads on Feb. 27, OPM Director Dale Cabaniss highlighted five assessments that agencies should use when determining an applicant's technical abilities: cognitive ability, structured interviews, biodata tests, situational judgment tests, personality tests, and training and experience point methods.

OPM has told agencies to use “a whole person approach” for assessing which current federal employees would be good candidates for retraining to fill high-demand cybersecurity jobs, taking into account “cognitive and interpersonal competencies, as well as technical cybersecurity related knowledge, skills, and abilities.”

Reference Links

- [OPM overhauls assessments for identifying cyber talent](#)
 - [America's Cybersecurity Workforce Executive Order 13870 Cybersecurity Aptitude Assessment Identification](#)
 - [Want to be Reskilled for a Cyber Job? Here's What Agencies Are to Look For](#)
 - [OPM's latest attempt to address cyber worker shortage focuses on testing](#)
-

Pentagon

Senate Armed Services Committee Tasks Pentagon's Principal Cyber Advisor with Cyber Pilot Program Responsibilities

Introduced – June 2020

Summary

The Senate Armed Services Committee wants to add new responsibilities to the Pentagon's Principal Cyber Advisor as part of a broader effort to ensure cyber forces can meet new challenges. The committee released a summary June 11 of the annual defense policy bill for fiscal year 2021. The passed bill adopts several recommendations made by the Cyberspace Solarium Commission, a bipartisan organization created in 2019 to develop a multipronged U.S. cyber strategy.

Among items the panel approved is giving the Principal Cyber Advisor more responsibility related to integration and coordination to ensure that DoD's cyber policies are coherent and cohesive. The bill includes several provisions to improve the way DoD procures cyber equipment as well as to improve the Congressional oversight of those programs.

The bill also requires the Department of Defense to launch pilot programs, demonstrations and/or plans around speed-based cybersecurity capability metrics to measure DoD performance and effectiveness, interoperability and automated orchestration of cybersecurity systems, addressing network timing and inconsistencies and integration of user activity monitoring and cybersecurity systems.

Reference Links

- [Senate committee wants more cyber pilot programs](#)
-

DARPA Issues Bug Bounty Challenge

Introduced – June 2020

Summary

DARPA issued a July bug bounty contest as part of its System Security Integration Through Hardware and Firmware (SSITH) program. The challenge focuses around electronic systems such as microchips, embedded devices, and hardware solutions.

Reference Links

- [DARPA Announces First Bug Bounty Program to Hack SSITH Hardware Defenses](#)
 - [Pentagon Issues Hacking Challenge](#)
 - [DARPA wants hackers to try to crack its new generation of super-secure hardware](#)
-

JAIC set to double its civilian workforce by FY 21 as automation gains momentum

Introduced – February 2020

Summary

Following the release of an AI playbook from the American Council for Technology-Industry Advisory Council, and less than a year after agencies joined forces to create both an artificial intelligence and robotic process automation community of practice, agency officials have expressed enthusiasm for this emerging technology, but agree that more steps are needed to scale up those applications. The JAIC currently has about 70 civilian staff and about 30-40 contract staff, but the agency expects to double its civilian workforce by the end of fiscal 2021.

Reference Links

- [JAIC set to double its civilian workforce by FY 21 as automation gains momentum](#)
-

JAIC and GSA Reaching out on 'Discovery Sprint'

Introduced – February 2020

Summary

The Defense Department's (DoD) Joint Artificial Intelligence Center (JAIC) and the General Services Administration's (GSA) Centers of Excellence (CoE) expect to reach out to Joint Common Foundation (JCF) stakeholders to set up one-on-one engagements on a "discovery sprint" that looks to accelerate and expand AI adoption.

The nine-month-long discovery sprint was announced in 2019 and will expand AI adoption in the DoD and across the Federal government.

Reference Links

[JAIC and GSA Reaching out on 'Discovery Sprint'](#)

White House

White House signs executive order protecting U.S. bulk power system

Introduced – May 2020

Summary

President Trump signed an executive order prohibiting bulk power system equipment from foreign companies that his administration believes could put the U.S. electricity system at risk. The Executive Order authorizes U.S. Secretary of Energy Dan Brouillette to work with the Cabinet and energy industry to secure America's bulk-power system.

Reference Links

- [Trump declares national emergency over threat to power system](#)
 - [White House signs executive order protecting U.S. bulk power system](#)
 - [U.S. president gives DOE control of determining bulk-power equipment purchases](#)
 - [What's Next for the Executive Order on Bulk-Power System Equipment?](#)
 - [The President's Executive Order on Grid Security Creates Peril and Uncertainty for US Power Companies](#)
 - [Implications of the Bulk-Power System Electrical Equipment Executive Order on energy infrastructure transactions](#)
 - [Executive Order Establishes New Challenges for Utilities](#)
 - [Trump's Order to Secure Power System Met with Favor, Uncertainty in Utility Industry](#)
-

White House Unveils National Strategy to Secure 5G

Introduced – April 2020

Summary

The national strategy document contains four lines of effort that the administration should undertake to ensure 5G security. The document lays out the vision that will guide the development, deployment, and management of secure and reliable 5G communications infrastructure worldwide of the U.S. together with that of its closest allies.

The document also addresses the steps the government should take which include efforts to facilitate the domestic rollout of 5G; assess the risks and identify the core security principles of 5G infrastructure; assess the risks to U.S. economic and national security during development

and deployment of 5G infrastructure worldwide, and promote responsible global development and deployment of 5G infrastructure.

Reference Links

- [National Strategy to Secure 5G](#)
 - [White House Unveils National Strategy for 5G Security Concurrently With Signing of the Secure 5G Act](#)
 - [White House strategy paper to secure 5G envisions America leading global 5G development](#)
-

White House Considering Space Cybersecurity Policies

Introduced – March 2020

Summary

The National Space Council is weighing a new policy directive that would call for the space industry to voluntarily adopt cybersecurity standards to help protect data and companies' intellectual property. The White House focus over the past year with regard to space policy has been on "supply chain hygiene." The administration would like to raise awareness about hackers trying to target satellite networks and industrial spies stealing U.S. space technology. Further, to increase supply chain security, the administration would like U.S. companies to reduce their dependence on foreign suppliers and, when domestic sources are not available, make sure that suppliers are certified.

Reference Links

- [White House might consider space policies on cybersecurity, supply chain, nuclear power](#)
 - [White House to Soon Release New Guidance for Cybersecurity in Space](#)
-

Executive Order instructs agencies to prepare for GPS outage

Introduced – February 2020

Summary

President Donald Trump issued an executive order detailing a series of deadlines to protect positioning, navigation and timing services and the associated critical infrastructure. The White

House directed agencies to take initial steps to protect GPS systems in a more whole of government approach.

- The departments of Commerce, Defense, Transportation and Homeland Security are considering how best to secure the systems that support global positioning satellites and related critical infrastructure.
- The National Institute of Standards and Technology announced a one-year deadline to develop foundational cybersecurity profiles to help manage risks to systems, networks and assets that depend on positioning, navigation and timing services.
- The Federal Acquisition Regulations Council also will develop new rules for products and systems that use GPS and similar services.

Reference Links

- [Executive Order on Strengthening National Resilience through Responsible Use of Positioning, Navigation, and Timing Services](#)
 - [Agencies ordered to prepare for GPS outage](#)
 - [Trump directs U.S. government agencies to protect critical infrastructure that relies on GPS](#)
 - [EO seeks to secure services such as GPS](#)
-

White House releases 2021 Budget Proposal Introduced – February 2020

Summary

The Office of Management and Budget (OMB) released the president's Fiscal Year 2021 budget proposal of \$4.8 trillion, which includes billions slotted for cyber investments at the Departments of Defense (DoD), Homeland Security (DHS), Energy (DoE), and Veterans Affairs (VA) and other agencies.

- The request includes \$14 billion for research and development (R&D) in artificial intelligence (AI), quantum information systems, 5G, cybersecurity, and other technological efforts.
- DoD's budget also includes \$10 billion for cyber investments in safeguarding DoD networks and information, supporting military commander objectives, and defending the nation.
- OMB budgeted DHS about \$1.1 billion for all cybersecurity efforts. At that level, the budget document says DHS could increase the number of network risk assessments it

leads from 1,800 currently to more than 6,500 going forward, and said some of those could support state and local election systems. The funding also would support the EINSTEIN and Continuous Diagnostics and Mitigation programs.

- The FY2021 budget request also supports DHS's Cyber Talent Management System, and a Cybersecurity and Infrastructure Security Agency (CISA)-led cybersecurity training program for all Federal employees.
- The administration budget proposal would also shift Secret Service from DHS to the Department of the Treasury in order to improve cybercrime investigations.
- \$4.9 billion is allocated to the VA in the FY2021 presidential budget proposal. The level of funding would support implementation of the MISSION Act, claims processing, supply chain management, and financial management business transformation. More than \$310 million is budgeted for cloud migration and aging infrastructure replacement to support VA's new electronic health records systems.
- DoE is allotted \$185 million for its Office of Cybersecurity, Energy Security, and Emergency Response, a \$29 million increase from last year. The money will be put toward early-stage R&D projects that improve cybersecurity and resiliency in the energy supply chain, the budget document says. The agency's new AI and Technology Office is slated to receive \$5 million in FY2021.
- The Federal Citizens Service Fund is allotted \$58.4 million to assist Federal agencies using cloud technologies and promote FedRAMP-authorized services;
- The National Institutes of Standards and Technology is allotted \$718 million – \$282 million less than FY20 – to advance U.S. innovation and technological development in AI, quantum information science, advanced manufacturing, and next generation communications technologies;
- The National Telecommunications and Information Administration is allotted \$25 million to modernize spectrum management systems and prepare for 5G;
- The Internal Revenue Service is allotted \$300 million to modernize its IT services and improve taxpayer experience and security; and
- The Department of Agriculture's rural broadband program received \$305 million less than FY20.

Reference Links

- [President's FY2021 Budget Prioritizes DoD, DHS, and VA Tech Investments](#)
 - [Here's what the White House wants to spend on IT](#)
 - [Cyber snippets from Trump's budget](#)
 - [Federal Tech Guide to Trump's 2021 Budget](#)
-

Secret Service may rejoin Treasury to improve cybercrime investigations

Introduced – February 2020

Summary

The proposed 2021 budget would shift the Secret Service from DHS to the Department of the Treasury in order to improve cybercrime investigations. The agency has been under Department of Homeland Security since it moved there after the 9/11 attacks.

Reference Links

- [Secret Service May Leave Homeland Security, Rejoin Treasury](#)
 - [White House budget plan has Secret Service back under Treasury](#)
-