May 2019

THE ICIT FEDERAL CYBERSECURITY 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

May 2019

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

www.icitech.org

Contents

About this Report

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

Readers should note the following:

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

Census Bureau

GAO Identifies Cybersecurity Issues For Upcoming Census

Introduced – May 2019

Summary

The GAO released testimony in early May expressing concern about the cybersecurity of the upcoming census and recommending that the Census Bureau "better ensure that cybersecurity weaknesses are addressed within prescribed time frames" and "improve its process for addressing cybersecurity weaknesses identified by [the Homeland Security Department]."

Reference Links

- GAO Flags New Cybersecurity Issues for Upcoming Census
- 'Significant work' remains for Census to address IT, cybersecurity ahead of 2020
- GAO urges Census Bureau to stay on track with cybersecurity to-do list

---

Census Bureau Increases System and Data Security

Introduced – April 2019

Summary

The Census Bureau is working on a revised methodology for maintaining data anonymity and it is increasing system security in anticipation of the 2020 decennial count.

Reference Links

- Census Bureau works on methodology for maintaining anonymity
- Census Bureau counts on new cybersecurity concerns

CIO Council

The Cyber Reskilling Academy Opened Its Second Round of Applications

Introduced – April 2019

Summary

The Reskilling Academy opened applications from late April through May 15. The reskilling academy will select participants starting in early June. Eight weeks of in-classroom training will run from July 8 through September 20. Unlike with the first cohort, which was open to all federal employees who don't currently work in the IT field, the second round was open to the entire workforce.

Reference Links

- Reskilling academy opens up new round of applications, as agencies seek more IT workforce investments

---

Federal Cyber Reskilling Academy Increasing Class Size

Introduced – April 2019

Summary

More than 1,500 applications has led the Federal Cyber Reskilling Academy to consider expanding class sizes and virtualization options.

Reference Links

- Demand pushes CIO Council to increase class size of cyber reskilling academy
- More than 1,500 feds applied for first Cyber Reskilling Academy cohort

Department of Defense (DOD)

JAIC Ramps Up Its Work

Introduced – April 2019

Summary

The Pentagon's Joint Artificial Intelligence Center (JAIC) is adding two new areas of focus—cybersecurity and robotic process automation—and expanding its outreach to academics and foreign allies.

Reference Links

- DOD's New AI Center Ramps Up

DOD is Considering Releasing Software Blacklist

Introduced – May 2019

Summary

The Defense Department wants to publish its blacklist of software companies to better inform the industrial base. It is currently working with Congress on authorization.

Reference Links

- DOD considers releasing list of blocked software vendors
- DOD looks to publish software blacklist

DOD Revises Acquisition Process

Introduced – May 2019

Summary

The Defense Department is pursuing acquisition improvements to improve the effectiveness of its solicitation processes, to advance the cybersecurity of needed solutions, and to meet rising adversarial threats, through initiatives such as Deliver Uncompromised and third-party supply chain security requirements.

Reference Links

- DOD Targets Acquisition Reform
- Pentagon eyes tougher contracting language for cyber, supply-chain security

- New Pentagon Initiatives Address Cybersecurity Challenges, Industrial Base Fragility
- DOD Steps Up Supply Chain Security Programs for Smaller Contractors
- DoD thinking of ways to implement 'deliver uncompromised' initiative

---

DOD Developing a Secure 5G Mobile Telecommunication Network Strategy

Introduced – May 2019

Summary

The Defense Department is developing a secure 5G mobile telecommunication network strategy to preempt threats to the emerging 5G technologies.5G networks would dramatically improve military communication and situational awareness, would be 100 times faster than current networks, and would be more resilient and less susceptible to attacks.

Reference Links

- DOD Develops Secure 5G Mobile Telecommunication Network Strategy
- THE 5G ECOSYSTEM: RISKS & OPPORTUNITIES FOR DoD

DOD Released Annual Report to Congress on the Military and Security Developments Involving the People's Republic of China

Introduced – May 2019

Summary

The Department of Defense released its annual report to Congress on the Military and Security Developments Involving the People's Republic of China ("PRC"), detailing the DoD's assessment of Chinese security strategy and military strategy over the next 20 years, with a particular focus on China's future course of military-technological developments.

Reference Links

- Department of Defense Releases Annual Report to Congress on the Military and Security Developments Involving the People's Republic of China
- ANNUAL REPORT TO CONGRESS: Military and Security Developments Involving the People's Republic of China 2019

DOD Proposes Appointing Senate-Confirmed IT officials for Army, Navy, Air Force

Introduced – May 2019

Summary

The Pentagon is preparing a legislative proposal that would require the Army, Navy, and Air Force to appoint a new senior, Senate-confirmed assistant secretary to handle information technology issues.

Reference Links

- DoD proposal would establish new Senate-confirmed IT officials for Army, Navy, Air Force
- Navy may restructure its IT org chart for second time in a year

---

Cyber Command Moving Towards "Defend Forward" Model

Introduced – May 2019

Summary

US Cyber Command may shift its strategy concerning foreign networks to continuous probing, otherwise referred to as "defend forward" so that they may preemptively detect adversarial activity on foreign networks.

Reference Links

- Cyber Command paying closer attention to overseas networks in its national defense mission
- DoD, DHS reach accord on new steps to cooperate in cyber defense

---

Pentagon Launches Allied Prototyping Initiative

Introduced – May 2019

Summary

The Defense Department's research and engineering arm has established an "Allied Prototyping Initiative" to collaborate with foreign partners on DOD's top technology goals, including hypersonic weapons, artificial intelligence and cybersecurity.

Reference Links

Pentagon to prototype key technologies with allies through new initiative

---

DoD JEDI Cloud Initiative Overcomes one Hurdle, Encounters Another

Introduced – April 2019

Summary

The DoD investigation concluded that at least two former employees, who previously had worked at or had ties to Amazon Web Services, had "no adverse impact on the integrity of the acquisition process." However, the investigation also uncovered potential ethical violations that have been referred to the DoD Inspector General.

Reference Links

- DoD's JEDI cloud effort clears internal review hurdle, but path forward remains rocky
- Watchdog group: DoD's JEDI cloud is mired in murk

The Air Force Announced Adoption of Cloud-Oriented Cybersecurity Strategy

Introduced – April 2019

Summary

The Air Force is refining new cloud-oriented cybersecurity technologies to safeguard vulnerable data networks and strengthen defenses against increasingly sophisticated AI-enabled cyber-attacks. The strategy includes multi-mode authentication techniques, software-reliant network upgrades, new patches and new cyber defenses fortified by the latest AI-related innovations.

Reference Links

- The Air Force Has a New Cyber Security Defense Plan
- Cloud will mean better cybersecurity for sensitive DOD data, deputy CIO says

---

Air Force Sets Up ATO Fast Track

Introduced – April 2019

Summary

The Air Force is piloting a new way to give systems an authority to operate (ATO) in just weeks by balancing rapid deployment with risk assessment. Essentially Fast Track is a combination of existing processes: systems must meet a cybersecurity baseline, plus include penetration testing and continuous monitoring.

Reference Links

- Cybersecurity ATOs, faster: Air Force sets up new Fast Track
- Air Force joins growing list of agencies paving a new cyber-approval path

---

DoD Plans to Begin Auditing Contractor Cybersecurity by 2020

Introduced – April 2019

Summary

The Department of Defense is developing metrics and establishing relationships with third-party auditors in anticipation of measuring contractor cybersecurity as part of the acquisition process, within the next 18 months.

Reference Links

- DOD likely to begin auditing contractors on cybersecurity in 2020
- Pentagon hopes to have new cybersecurity standards for contractors in 2020
- DoD will crack down on contractors not complying with cybersecurity standards

---

GAO Identifies Cybersecurity Open Priority Recommendations for DoD

Introduced – April 2019

Summary

The Government Accountability Office (GAO) identified 91 open priority recommendations to the Defense Department (DoD) – the highest number outstanding for all Federal agencies – with cybersecurity as one of the nine major areas DoD should prioritize

Reference Links

- Cyber Issues High On GAO's Fix-It List for DoD
- GAO Issues New Priority Recommendations for Defense Department

---

The Defense Health Agency (DHA) Migrated to the Cloud

Introduced – April 2019

Summary

The Defense Health Agency (DHA), which enables the military to provide medical services to combatant commands during both peacetime and wartime, has migrated to the cloud using General Dynamics Information Technology (GDIT) to migrate its Armed Forces Billing and Collection Utilization Solution

(ABACUS) to Amazon Web Services (AWS) GovCloud Region under the GSA IT Schedule 70 contract vehicle.

Reference Links

- Defense Health Agency Moves to the Cloud
- The Healthcare Cloud and Defense Health Agency: The What, Why, and When

---

DOD Artificial Intelligence Strategy Released

Introduced – February 2019

Summary

The Department of Defense released a roadmap for how the military will adopt AI and machine learning in future cyber operations, with a focus on defensive cybersecurity for hardware and software platforms.

Reference Links

- What the Pentagon's new AI strategy means for cybersecurity
- SUMMARY OF THE 2018 DEPARTMENT OF DEFENSE ARTIFICIAL INTELLIGENCE STRATEGY
- DOD artificial intelligence strategy seeks to address cybersecurity concerns

---

DOD Tightened Contractor Cyber Regulations

Introduced – November 2018 - February 2019

Summary

Over the last three months, the Department of Defense released new guidance and memos instructing contractors on how to improve their cybersecurity and cyber-hygiene practices, or else risk losing business with the Pentagon.

Reference Links

- DoD tightens enforcement of cyber regulations on contractors to protect data
- GUIDANCE FOR ASSESSING COMPLIANCE OF AND ENHANCING PROTECTIONS FOR A CONTRACTOR'S INTERNAL UNCLASSIFIED INFORMATION SYSYEM
- DoD Guidance for Reviewing System Security Plans and the NIST SP 800-171 Security Requirements Not Yet Implemented

- DOD to require 'enhanced' cyber protections from contractors working on 'critical' programs
- Pentagon developing plan to grade contractors on 'cyber score'

Department of Defense Unveils Cloud Strategy, JEDI

Introduced – February 2019

Summary

The DOD cloud strategy details the Joint Enterprise Defense Infrastructure cloud initiative known as JEDI. The JEDI program is the "foundational approach to deliver the benefits of a General Purpose enterprise cloud for DoD." The strategy emphasizes a cloud hierarchy at DOD, with JEDI on top and MilCloud second in command, followed by multiple "fit-for-purpose" clouds.

Reference Links

- DOD's leads cloud strategy with JEDI
- DoD Publishes Cloud Strategy With Eye on Modernization
- Unclassified: DoD cloud strategy to focus on AI adoption
- A tweaked DoD cloud strategy looks beyond Amazon

Defense Information Systems Agency

DISA Projected to Expand by 1,200 Employees and $1B Workload by 2020

Introduced – April 2019

Summary

The Defense Information Systems Agency will officially takes responsibility for running much of the information technology that supports the 28 agencies in DoD's "fourth estate" by 2020. It's workforce is predicted to increase by 1,200 new employees as its workload increases by nearly $1 billion.

Reference Links

- DISA to take on 1,200 new employees, nearly $1B workload in 2020

DISA Calls for Industry to Build Transparency into Artificial Intelligence

Introduced – February 2019

Summary

Vice Adm. Nancy Norton, USN, director of the Defense Information Systems Agency (DISA) and commander, Joint Force Headquarters–Department of Defense Information Network (JFHQ-DODIN), called on industry to improve the transparency and resiliency of AI systems during his keynote luncheon address at the AFCEA Rocky Mountain Cyberspace Symposium.

Reference Links

DISA Calls on Industry to Build Transparency into Artificial Intelligence

Department of Energy (DOE)

GAO Recommends DOE Prioritize IT and Nuclear Modernization

Introduced – April 2019

Summary

In the Government Accountability Office (GAO) letter of open priority recommendations for the Energy Department (DoE), nuclear modernization, aging legacy IT systems, and cybersecurity featured among the seven major areas GAO highlighted.

Reference Links

- GAO Flags IT and Nuclear Modernization Among DoE Priorities

---

DOE Invests in Quantum Research

Introduced – April 2019

Summary

The Department of Energy plans to spend $40 million in research funding to develop new algorithms and software for quantum computers. The plan would fund large, multidisciplinary teams to dramatically accelerate development of software adaptable to a range of different quantum computing systems as well as a wide variety of potential applications. DOE intends to make two sets of awards – one to universities, industry and nonprofits, and one to national lab teams. Two to three collaborative teams will be funded at between $250,000 and $2,500,000 per year, over five years, subject to appropriations.

Reference Links

- DOE dials up funding for quantum research
- Department of Energy to Provide $40 Million to Develop Quantum Computing Software

---

DOE Announces $70M for Cybersecurity Institute for Energy Efficient Manufacturing

Introduced – April 2019

Summary

The US Department of Energy (DOE) announced up to $70 million for a Clean Energy Manufacturing Innovation Institute to develop technologies that will advance US manufacturing competitiveness,

energy efficiency, and innovation. This Institute will focus on early-stage research for advancing cybersecurity in energy efficient manufacturing.

Reference Links

- DOE announces $70M for Cybersecurity Institute for Energy Efficient Manufacturing
- Energy Department announces $70M for advancing cybersecurity in energy efficient manufacturing
- DOE Pledges $70 Million Toward Energy Efficient Manufacturing

---

DOE Announced $20 million Investment in AI and Machine Learning Tools

Introduced – April 2019

Summary

The U.S. Department of Energy's (DOE's) Advanced Research Projects Agency-Energy (ARPA-E) announced up to $20 million in funding to accelerate the incorporation of machine learning and artificial intelligence into energy technology and product design processes.

Reference Links

- Department of Energy Announces $20 Million to Develop Artificial Intelligence and Machine Learning Tools
- DOE to Explore AI that Can Secure Power Grid

DOE Awards $36 Million to Increase Solar Grid Cyber Resilience

Introduced – April 2019

Summary

The US Department of Energy (DOE) has selected up to $36 million in research projects that will advance solar energy's role in strengthening the country's grid resilience.

Reference Links

- US DOE awards $36 million to solar-based grid resilience projects
- Advanced Systems Integration for Solar Technologies (ASSIST): Situational Awareness and Resilient Solutions for Critical Infrastructure

---

DOE Announces Cybersecurity Institute for Energy Efficient Manufacturing

Introduced – February 2019

Summary

The US Department of Energy's (DOE's) Office of Energy Efficiency and Renewable Energy (EERE) will issue a Funding Opportunity Announcement (FOA) entitled "Clean Energy Manufacturing Innovation Institute: Cybersecurity in Energy Efficient Manufacturing." The FOA establishes a new Clean Energy Manufacturing Innovation Institute to develop technologies that will advance US manufacturing competitiveness, energy efficiency, and innovation. The Institute, will focus on Cybersecurity in Manufacturing—understanding the evolving cybersecurity threats to greater energy efficiency in manufacturing industries, developing new cybersecurity technologies and methods, and sharing information and expertise to the broader community of US manufacturers.

Reference Links

- DOE to establish a cybersecurity institute for energy efficient manufacturing
- DOE to create clean energy manufacturing innovation institute
- DOE targets growing cyber threats to more efficient manufacturing
- DOE to fund cybersecurity for new Clean Energy Manufacturing Innovation Institute

---

DOE Announces $40 Million for Grid Modernization Initiative

Introduced – February 2019

Summary

DOE Under Secretary of Energy Mark Menezes announced that $40 million in FY19 funding for the Grid Modernization Initiative (GMI). The GMI focuses on working with public and private partners to develop new tools and technologies that measure, analyze, predict, protect, and control the grid of the future.

Reference Links

- DOE Announces $40 Million for Grid Modernization Initiative
- DOE Allots $40M for Grid Modernization Projects

DOE and FERC to Discuss Best Practices and Increasing Investment in Energy Systems in Response to Cyber Threats

Introduced – February 2019

For More Information on Receiving the Monthly ICIT Federal Agency Initiatives Analyst Report

contact ICIT at

info@icitech.org