September 6, 2017

Hacking Healthcare

TLP White
Policy Analysis – Who does what (pt. 2)

This week we will wrap up our review of different federal agencies with a cybersecurity mission. Last week we looked at how DHS and FBI work to protect and support U.S. interests in the face of cyber-threats. Today we will look at HHS's role as well as the other agencies that contribute legal authorities and cyber-capabilities to the U.S. government's "defensive" cyber-mission. We will also do a quick overview of the agencies responsible for the government's "offensive" activities in cyber-space and give you a sense of the doctrine that helps determine how it is applied.

HHS has three cybersecurity missions that have been authorized and funded by Congress – defend its own networks and data; support the health care sector; develop and enforce regulations. The new Health Cybersecurity and Communications Center (HCCIC) has a role to play in executing responsibilities in line with all three mission areas. As we described in a previous edition of the newsletter, the HCCIC will serve to integrate SOC functions across the different HHS bureaus, lend health sector specific expertise to threat intelligence analysis at the six cyber centers (specifically the NCCIC), and inform the long-term development of regulatory policy to reflect the nature of the cyber threat against the healthcare sector.

Planning for public health emergencies is conducted within HHS by the Assistant Secretary for Preparedness and Response (ASPR), who is also responsible for carrying out the role of "sector-specific agency." The role of a sector specific agency (created under PPD-21) is to support the resiliency of the health care sector from within the federal government. This includes lending sector relevant expertise to other agencies around the government, such as DHS, the FBI, or the intelligence community, as well as serving as an interface between the government and private sector personnel during both steady-state and incident response.

HHS' regulatory authorities sit within a few different offices – the Office of Civil Rights (OCR) and the Food and Drug Administration (FDA), as well as the Office of the National Coordinator for health IT (ONC) and the Centers for Medicare & Medicaid Services (CMS). Congress gave OCR the authority to implement and enforce HIPAA, which sets expectations for how health organizations protect patient information. FDA sets the regulations by which medical devices must comply and has issued both pre- and post-market guidance for the cybersecurity of medical devices. ONC and CMS are not regulators in the traditional sense, but both oversee federal subsidy programs and set "regulatory" requirements that health care organizations must meet in order to receive benefits. ONC (for "Meaningful Use") and CMS (for Medicare/Medicaid), both expect participants to appropriately manage cyber risks.

September 6, 2017

Beyond DHS, FBI, and HHS, there are a few other health sector relevant agencies that play a role in cybersecurity.

The Department of Commerce sets standards for federal government agencies through the National Institute of Standards and Technology (NIST), which in recent years has extended that expertise to develop frameworks of standards and best practices for private entities to adopt (most notably the CSF, but more recently the NICE Framework). NIST also funds and conducts research in cybersecurity, including applied research at the National Cybersecurity Center of Excellence, as well as managing the National Vulnerability Database. The Department of Commerce is also responsible for the National Telecommunications & Information Administration, which primarily manages spectrum allocation for the government, but also has broad responsibility for Internet policy and has in recent years led a number of multi-stakeholder processes to inform development of that policy. One current multi-stakeholder process is related to the security of Internet of Things devices.

The Federal Trade Commission (FTC) and Federal Communications Commission (FCC) are both regulatory agencies with purview over cybersecurity matters and a voice in government policy development. FTC has authority to enforce a number of consumer protection laws, including those related to unfair and deceptive practices. This authority has been used recently against companies such as UBER, which "failed to live up to its claims" of monitoring access to rider and driver data and appropriately securing that data. The FCC is responsible for ensuring the availability and resilience of the nation's telecommunications infrastructure and in that role sets regulatory expectations of telecommunications companies, as well as working with DHS in a sector-specific capacity.

The National Security Agency (NSA) also plays a role in the government's defensive mission. The Information Assurance Directorate (IAD) is responsible for securing the government's national security systems – in other words, those that conduct classified activity or store classified information. NSA is also authorized, under certain circumstances to lend expertise to critical infrastructure companies in the form of technical assistance. This technical assistance is usually obtained through a request made by HHS, in its role as sector-specific agency, or DHS.

To conduct this defensive mission, NSA draws on the cryptographic and cyber-exploit capabilities that it has developed for its role in signals-intelligence and offensive cyber operations. NSA collects foreign "signals" related to certain foreign individuals of interest or foreign-born threats against U.S. persons. NSA also supports Cyber Command and other DOD missions as they look to conduct network operations against military targets. Cyber Command is currently led by Admiral Rogers, who is "dual hatted" and also leads NSA.

DOD's cyber-mission is, as you would imagine from such a large organization, multi-faceted. Military services such as the Army and Navy utilize cyber capabilities to conduct in theatre intelligence collection and support kinetic operations. But DOD also supports the defense industrial base (DIB) as a sector of the economy's critical infrastructure. In fact, one of DOD's cyber centers – DC3 – may serve as an appropriate model as HCCIC looks to support the health care industry. And the Air Force Office of Special Investigations has the capabilities and authorities to investigate and mitigate cyber-threats against DOD, the DIB, and the U.S. Government. Importantly for the health care sector, this include the Defense Health Agency and the health care delivery units within each service branch.

CIA puts cyber capabilities to use as they conduct intelligence collection and other foreign operations in line with their authorized mission.

September 6, 2017

The National Security Council's Cybersecurity Directorate directly supports the President's ability to utilize the government's cyber capabilities and authorities when making decisions and directing actions. To do that, NSC coordinates agency actions and leads processes to develop supporting policies and procedures. In certain cases, such as its role in incident response – which we previously discussed, the NSC will actually lead operational decision making. One example of the NSC exerting operational leadership during steady state situations is the Vulnerability Equities Process, which determines when and how the government will disclose vulnerabilities in commercial software and hardware.

That wraps up our overview of all the different moving pieces within the government's cyber-apparatus.

Next week we will plan to look at all the cybersecurity legislation that may come before Congress this fall.

Hot Links **– NH-ISAC is currently tracking activity related to Hurricane Harvey.**

FDA today releases its final guidance on the interoperability of medical devices. This guidance considers security, but does not depart in scope or tone from the premarket cybersecurity guidance that FDA has previously released. For example, "FDA recommends that manufacturers include … a particular focus on … security issues introduced when including an electronic interface." This seems like the reasonable, if not groundbreaking, approach that one would hope the regulators put forward. Here's a blog post from the lead author of the guidance.

Taking Stock of Trump's Cybersecurity Executive Order So Far (Wired)
The American Technology Council releases its draft IT modernization strategy (Federal News Radio)
McCaskill, Johnson Request Details on Cybersecurity Plans Following President Trump's Executive Order (Senate Homeland Security)
Hackers volunteer to help those affected by Hurricane Harvey (CW39)
Amazon S3 Bucket Leaks Expose Classified US Veteran Data (Dark Reading)
Who Is Marcus Hutchins? (Krebs)

The Week Ahead –

Administration activity –

--NTIA will host a meeting of its multi-stakeholder process on the security of IoT devices. This one takes place in New York and looks at upgradability and patching. (9/12)

Congressional Activity – The House and Senate are back in session after the August recess. Lots of activity in committee hearings.

Wednesday, September 6:
--Confirmation hearing – Matthew Bassett to be HHS Assistant Secretary for Legislation (Senate Finance)
--Hearings to examine the history and current reality of the United States health care system. (Senate Homeland Security)
--Stabilizing Premiums and Helping Individuals in the Individual Insurance Market for 2018: Health Care Stakeholders (Senate HELP)

September 6, 2017

Thursday, September 7:
--Appropriations Hearing – HHS 2018 Appropriations markup (Senate HELP)
--Stabilizing Premiums and Helping Individuals in the Individual Insurance Market for 2018: Health Care Stakeholders (Senate HELP)
--Hearing to examine Navy Readiness in light of the USS Fitzgerald and USS McCain (House Armed Services)
--Challenges of recruiting and retaining a cybersecurity workforce (House Homeland)

Tuesday, September 12:
--Hearing on "The Dynamic Gains from Free Digital Trade for the U.S. Economy" (Joint Economic Committee)
--Resiliency: The Electric Grid's Only Hope (House Science, Space, and Technology)
--21st Century Trade Barriers: Protectionist Cross Border Data Flow Policies Impact on U.S. Jobs (House Energy and Commerce)

Conferences and Webinars –
--Basic Best Practices in Cybersecurity – Minnesota (NH-ISAC) (9/6)
--Medical Device Workshop at Medtronic – Mounds View, MN (NH-ISAC) (9/7)
--HIMSS Healthcare Security Forum (9/11-13)
--NTIA Security of IoT devices multi-stakeholder process (9/12)
--Billington CyberSecurity Summit (9/13)
--Basic Best Practices in Cybersecurity - Alabama (NH-ISAC) (9/15)
--Biotec/Pharma Security Workshop at MSD, Prague (NH-ISAC) (11/7)
--NH-ISAC Fall Summit – Cyber Rodeo (11/28-30)

Reports –
--The SANS 2017 Data Protection Survey (SANS)

Podcasts –
Steptoe Cyberlaw Podcast: Interview with Michael Mainelli (lawfare) – a good dive into a few big stories from August – Kaspersky; Apple's vulnerabilities and China VPN policy, IoT Security; UK data protection law; election hacking; bitcoin, blockchain, etc.

Sundries –
Policy:
--Justice Department: 'Legislation may be necessary' if companies do not turn over data (Washington Examiner)
--Kentucky HIPAA Violation Case Ruling Held by Appeals Court (Health IT Security)
--International Firms Struggle to Adapt as China's Cybersecurity Law Takes Shape (Dark Reading)
--UK Lawyer suggests tying access to encryption to verified ID (Naked Security)

Government Cybersecurity:
--Security Flaw in Estonian National ID Card (Schneier)
--How Las Vegas uses AI to protect against hackers (Nextgov)
--Cloud security is the future of government's hack protection (Federal News Radio)

September 6, 2017

Breaches:
--Judge Rules that Yahoo Breach Victims Can Sue (Dark Reading)

Op-eds:
--Why the US Government Shouldn't Ban Kaspersky Security Software (Wired)
--The real cost of alarm fatigue (HelpNet)
--New cyber regulations [in financial services] highlight need for virtual CISOs (CSO)
--3 Ways AI Could Help Resolve the Cybersecurity Talent Crisis (Dark Reading)
--Mikko Hypponen's Vision of the Cybersecurity Future (Dark Reading)

Tech:
--Security-focused phone launches crowdfunding drive (Naked Security)
--Google promised not to scan Gmail for targeted ads—but for how long? (Ars)

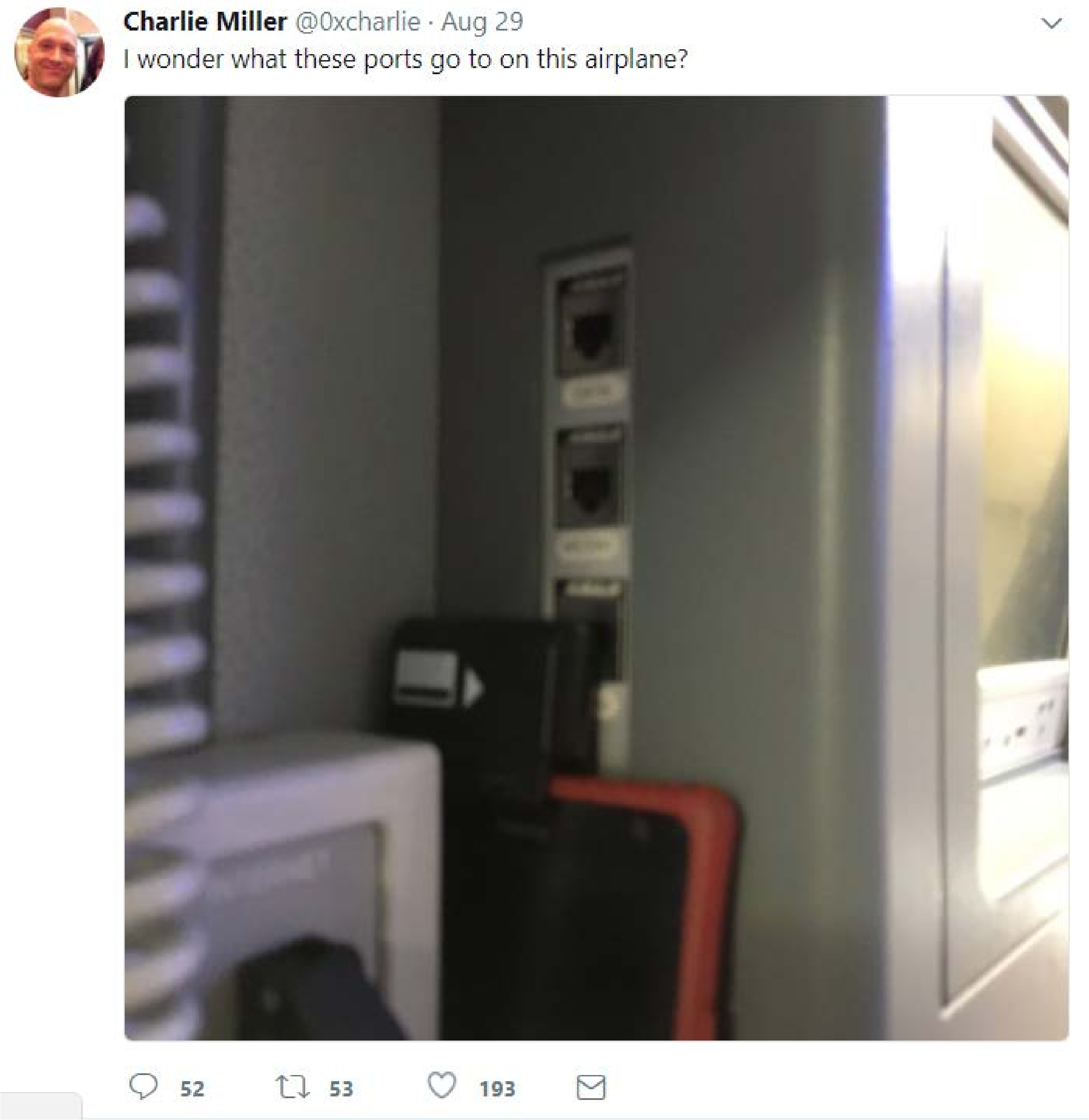
Threats:
--Ransomware scam spoofs FBI and IRS (Nextgov)
--Locky ransomware returns with new tricks up its sleeve (HelpNet)
--Researchers uncover latest version of Chinese spyware used to target dissidents (CyberScoop)
--Russian Hacking Tools Codenamed WhiteBear Exposed (Schneier)
--Scammers Are Exploiting Hurricane Harvey to Dupe Well-Intentioned Folks. (Fortune)
--Boston Red Sox caught red-handed using Apple Watch to steal signs (Ars)

Vulnerabilities:
--Firmware Update to Address Cybersecurity Vulnerabilities Identified in Abbott's (formerly St. Jude Medical's) Implantable Cardiac Pacemakers: FDA Safety Communication (FDA)
--Abbott Laboratories' Accent/Anthem, Accent MRI, Assurity/Allure, and Assurity MRI Pacemaker Vulnerabilities (ICS-CERT)
--Severe security vulnerability found in Apache Struts (lgtm)
--Patch released for critical Apache Struts vulnerability (Threat Post)
--Remember when Lenovo sold PCs with Superfish adware? It just got a mild scolding from FTC (the Register)
--Serious Flaws Found in Westermo Industrial Routers (Security Week)

Network defense:
--Researchers reverse 320 million hashed passwords (HelpNet)
--Explainer: What is DNS Hijacking? (Wired)
--Explainer: How to detect and remove a rootkit in Windows 10 (CSO)
--People with non-IT backgrounds could help fill cyber security skills gap (Computer Weekly)
--HackerOne Expects $100m Paid Out in Bounties by 2020 (info security)

***(In)Secure Takes* –** Twitter's best from the week

September 6, 2017



Charlie Miller @0xcharlie · Aug 29

I wonder what these ports go to on this airplane?

Contact us: follow @NHISAC and email at bflatgard@nhisac.org