**Hacking Healthcare**

**TLP White**

***Policy Analysis –***

This week, we will look at incident response policy. After all, August seems like a good month to revisit incident response plans. This will be the first stage in a multi-part series – today we will lay the ground work by reviewing how the federal government organizes itself to support cyber incidents that impact critical infrastructure. In future weeks, we will look at regulatory requirements under HIPAA and other statutes, as well as more closely examine the role NH-ISAC plays in incident response within the health care industry.

In 2016, the federal government released a policy to formalize incident response processes. [Presidential Policy 41: United States Cyber Incident Coordination](https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident) (PPD-41, for short) established a definition of cyber incidents, committed the government to core principles, defined different lines of effort, and created new coordinating structures.

To help clarify roles and responsibilities, the government came up with the concept of “concurrent lines of effort,” which would all be activated when responding to a *significant* cyber incident. **Threat response** (Led by FBI) is the work done to mitigate the threat, whether it be through law enforcement or disruptive operations. **Asset response** (led by DHS) focuses on defending IT assets and restoring services. This can involve sending technical staff to organizations that have been hacked, as well as analyzing and sharing information to limit impact within a firm or across a sector or region. **Intelligence support** (led by ODNI) includes building and sharing awareness of the threat. **Business response** is a fourth line of effort that is the responsibility of the victim of the attack. In the case of an attack against critical infrastructure, the agency responsible for the relevant sector will be responsible for serving as the federal coordinator with that entity. In the case of the healthcare sector, that’s HHS.

When a significant cyber incident occurs, two coordinating structures are *automatically* established. At the base level, a field-level coordination group will be established by the federal personnel that is in communication with a private entity. This is meant to enable a single federal voice and prevent confusion. A level up from the field, a Unified Coordination Group (UCG) will be formed. This will include senior cybersecurity officials from the agencies leading each line of response, as well as representatives from other required agencies. The CIO or CISO of a victim company, or the leadership of a relevant sector ISAC, might be invited to join this group.

If the UCG deems it necessary (or cabinet officials decide to intervene), a Cyber Response Group (CRG) will be formed to lead coordination out of the White House. The CRG is technically chaired by the President’s Homeland Security Council (currently Tom Bossert), but leadership may be deferred to the NSC Cyber Coordinator (currently Rob Joyce). This group is charged with ensuring that any risk to national security is fully considered and that necessary resources are deployed.

All of this says nothing of how regulators fit into the mix or what expectations they have of health care companies. Next week we’ll look into that.

***Hot Links* –**

--[A Candid Conversation with The White House’s Man on Cyber](https://www.thecipherbrief.com/column/state-secrets/candid-conversation-white-houses-man-cyber-1092) (Cipher Brief) -- Suzanne Kelly, the Cipher Brief’s CEO sat down with Rob Joyce, the NSC’s Cyber Coordinator (he replaced Michael Daniel who held the role under Obama). The full interview can be heard on the [podcast](https://www.thecipherbrief.com/podcasts/rob-joyce-white-house-cybersecurity), but the article gives a good high level view of the issues Rob is most focused on. Protecting critical infrastructure is at the top of his list – and he describes how the partnership with private industry needs to be more robust. The health sector has a role to play here, with NH-ISAC at the center of such a partnership. NH-ISAC’s work through its grant with HHS will be a central component to defining roles and responsibilities. An upcoming edition of the newsletter will cover the work from that grant in greater detail.

--[Does HIPAA need to be updated in light of the opioid epidemic?](https://healthitsecurity.com/news/do-hipaa-regulations-need-updates-on-patient-privacy) (Health IT Security) – Last week, [Secretary Price indicated](https://www.whitehouse.gov/the-press-office/2017/08/08/press-briefing-opioid-crisis-882017) (WH press briefing) that the Administration is discussing modifications to the HIPAA privacy rules that would make it easier for health care organizations to notify family members when a patient is treated for an overdose or other opioid related conditions.

--[Four Top Cybersecurity Officials Are Leaving US Government](https://www.buzzfeed.com/kevincollier/four-top-cybersecurity-officials-are-leaving-us-government?utm_term=.trYdZ3Go0#.pw02l8dk6) (BuzzFeed) – The trend we highlighted last week seems to be continuing, with the CIOs of the EPA, Navy, and OPM handing in their resignations.

--[E-prescription bill gains support](http://www.healthcareitnews.com/news/national-e-prescribing-bill-gains-support-trump-declares-opioid-state-emergency) (Healthcare IT News)

--[HHS HCCIC will improve healthcare cybersecurity](https://healthitsecurity.com/news/how-hhs-hccic-will-improve-healthcare-cybersecurity) (Health IT Security)

--[HCCIC takes a quantum leap forward to secure the Health Sector](http://icitech.org/hhs-hccic-takes-a-quantum-leap-forward-to-secure-the-health-sector/) (ICIT)

--[Getting Granular on Cybersecurity: Experts Talk Frameworks and Hacks in Philadelphia](https://www.healthcare-informatics.com/article/cybersecurity/getting-granular-cybersecurity-experts-talk-frameworks-and-hacks-philadelphia) (Healthcare Informatics)

--[Double role for White House cyber aide shows challenges for new administration](https://www.cyberscoop.com/double-role-white-house-cyber-aide-shows-challenges-new-administration/) (CyberScoop)

***The Week Ahead* –**

*Administration activity –* There are rumors that the Administration is getting ready to release a cyber deterrence strategy, but nothing has been made public as of now. Watch this space.

--[Fact Sheet: President Donald J. Trump Protects American Intellectual Property](https://www.whitehouse.gov/the-press-office/2017/08/14/fact-sheet-president-donald-j-trump-protects-american-intellectual) (WH)

*Congressional Activity –* The House and Senate are both in recess, though the Senate continues *pro forma* sessions, which means that recess appointments are unlikely. Both chambers are likely to return to business after Labor Day on September 5.

*Conferences and Webinars –*

--[HIPAA Hybrid Entities - What if Healthcare is only a part of what you do](http://www.mentorhealth.com/control/w_product/~product_id=801038LIVE?infosec-conferences.com_Aug_2017_SEO) (webinar) (8/17)

--[Basic Best Practices in Cybersecurity – Texas](https://nhisac.org/events/nhisac-events/basic-best-practices-in-cybersecurity-texas/) (NH-ISAC) (8/23)

--[HIPAA Training for the Business Associate](http://www.mentorhealth.com/control/w_product/~product_id=801043LIVE?infosec-conferences.com_Aug_2017_SEO) (webinar) (8/23)

--[HIPAA and Personal Devices](http://www.mentorhealth.com/control/w_product/~product_id=801044LIVE?infosec-conferences.com_Sep_2017_SEO) (webinar) (9/5)

--[Basic Best Practices in Cybersecurity – Minnesota](https://nhisac.org/events/nhisac-events/basic-best-practices-in-cybersecurity-minnesota/) (NH-ISAC) (9/6)

--[Medical Device Workshop at Medtronic – Mounds View, MN](https://nhisac.org/events/nhisac-events/nh-isac-mdiss-medical-device-cyber-security-workshop-sept-7/) (NH-ISAC) (9/7)

--[HIMSS Healthcare Security Forum](http://www.healthcaresecurityforum.com/boston/2017?utm_source=hitn&utm_medium=news&utm_term=ridge&utm_content=ridge&utm_campaign=register-now) (9/11-13)

--[Billington CyberSecurity Summit](https://www.billingtoncybersecurity.com/8th-annual-billington-cybersecurity-summit/) (9/13)

--[Basic Best Practices in Cybersecurity - Alabama](https://nhisac.org/events/nhisac-events/basic-best-practices-in-cybersecurity-alabama/) (NH-ISAC) (9/15)

--[NH-ISAC Fall Summit – Cyber Rodeo](https://nhisac.org/events/cyber-rodeo/) (11/28-30)

***Breaches –***

--[Nationwide settles 2012 breach](http://www.healthcareitnews.com/news/nationwide-pays-55-million-2012-breach-127-million-accounts) (Healthcare IT News)

--[Pacific Alliance Medical Center hit by ransomware attack](http://www.healthcareitnews.com/news/los-angeles-provider-potentially-breached-ransomware-attack) (Healthcare IT News)

--[Hackers breach third party cloud vendor TekLinks](http://www.healthcareitnews.com/news/hackers-breach-third-party-cloud-vendor-teklinks) (Healthcare IT News)

***Reports –***

--[2017 HIMSS Cybersecurity Survey](http://www.himss.org/2017-himss-cybersecurity-survey)

***Podcasts –***

--[Rob Joyce on White House Cybersecurity](https://www.thecipherbrief.com/podcasts/rob-joyce-white-house-cybersecurity) (Cipher Brief)

--[Improving Medical Device IOT](https://itunes.apple.com/us/podcast/healthcare-information-security-podcast/id504642987?mt=2#episodeGuid=https%3A%2F%2F0267f973c7f511eda6a4-193e28812cee85d6e20ea22afb83e185.ssl.cf1.rackcdn.com%2Fimproving-cybersecurity-iot-medical-devices-directLink-9-i-3665.mp3) (Healthcare Information Security Podcast)

***Sundries –***

*August Vacation reading:*

--[Breaches Are Coming: What Game of Thrones Teaches about Cybersecurity](https://www.darkreading.com/vulnerabilities---threats/breaches-are-coming-what-game-of-thrones-teaches-about-cybersecurity/a/d-id/1329595) (Dark Reading)

*Policy and government cybersecurity:*

--[OCR deputy: Have policies in place to avoid a HIPAA compliance review](http://www.healthcareitnews.com/news/ocr-deputy-have-policies-place-avoid-hipaa-compliance-review) (Healthcare IT News)

--[FTC Blogs Review Data Security, Data Breach Prevention Basics](https://healthitsecurity.com/news/ftc-blogs-review-data-security-data-breach-prevention-basics) (Health IT Security)

--[FTC “Stick with Security” Blog](https://www.ftc.gov/news-events/blogs/business-blog)

--[Trump can’t use cyber to stop North Korea’s nuclear weapons](https://www.wired.co.uk/article/us-cyber-war-against-north-korea) (Wired)

--[Former UK spy chief says encryption 'very positive' despite attacks](https://www.reuters.com/article/us-usa-china-southchinasea-exclusive-idUSKBN1AQ0YK?il=0) (Reuters)

--[Sec. Mattis visits Silicon Valley](https://www.wired.com/story/james-mattis-artificial-intelligence-diux/) (Wired)

--[Ukranian Police Arrest Suspect in Petya Ransomware Campaign](https://www.onthewire.io/ukrainian-police-arrest-suspect-in-petya-ransomware-campaign/) (on the wire)

--[China's three internet giants being investigated for content that 'endangers national security'](https://www.cnbc.com/2017/08/10/tencent-baidu-and-sina-under-investigation-for-cyber-security-violations.html) (cnbc)

--[Amid Washington Russia Frenzy, Kaspersky Faces Backlash](http://foreignpolicy.com/2017/08/11/amid-washington-russia-frenzy-kaspersky-faces-backlash/) (FP)

--[Here’s the Memo That Blew Up the NSC](http://foreignpolicy.com/2017/08/10/heres-the-memo-that-blew-up-the-nsc/) (FP)

*Op-eds:*

--[Cyber Threat or Cyber Threat Inflation? - Assessing the Risk to U.S. National Security](http://smallwarsjournal.com/jrnl/art/cyber-threat-or-cyber-threat-inflation-assessing-the-risk-to-us-national-security) (Small Wars)

--[Penn Medicine CIO calls for international law enforcement cooperation to fight cybercrime](http://www.healthcareitnews.com/blog/penn-medicine-cio-calls-international-law-enforcement-cooperation-fight-cybercrime) (Healthcare IT News)

--[The United States of Cyber Debility](https://www.thecipherbrief.com/article/exclusive/international/united-states-cyber-debility) (Cipher Brief)

--[Analyzing the Internet of Things Cybersecurity Improvement Act](https://www.aei.org/publication/analyzing-the-internet-of-things-iot-cybersecurity-improvement-act/) (AEI)

*Tech:*

--[Ethereum is coding’s new wild west](https://www.wired.com/story/ethereum-is-codings-new-wild-west/) (Wired)

--[Want a diagnosis tomorrow, not next year? Turn to AI](https://www.wired.com/story/ai-that-will-crowdsource-your-next-diagnosis/) (Wired)

--[Microsoft unveils open source Coco blockchain framework for healthcare, other industries](http://www.healthcareitnews.com/news/microsoft-unveils-open-source-coco-blockchain-framework-healthcare-other-industries) (Healthcare IT News)

--[Biohackers encoded malware in a strand of DNA](https://www.wired.com/story/malware-dna-hack/) (Wired)

*Network defense and threats:*

--[Amazon Tackles Security of Data in S3 Storage](https://www.darkreading.com/cloud/amazon-tackles-security-of-data-in-s3-storage-/d/d-id/1329628?) (Dark Reading)

--[Ransomware 2.0: It's coming, and healthcare needs to get prepared](http://www.healthcareitnews.com/news/ransomware-20-its-coming-and-healthcare-needs-get-prepared) (Healthcare IT News)

--[Microsoft finds critical wormable bug lurking in every version of Windows](http://www.healthcareitnews.com/news/microsoft-finds-critical-wormable-bug-lurking-every-version-windows) (Healthcare IT News)

--[Beware misconfiguration errors: Little slip-ups can have huge consequences](http://www.healthcareitnews.com/news/beware-misconfiguration-errors-little-slip-ups-can-have-huge-consequences) (Healthcare IT News)

--[71 Percent of Healthcare Organizations Allocate a Specific Budget to Cybersecurity](https://www.healthcare-informatics.com/news-item/cybersecurity/survey-71-percent-healthcare-organizations-allocate-specific-budget) (Healthcare Informatics)

--[What Are Critical Considerations in Risk Management?](https://healthitsecurity.com/news/what-are-critical-considerations-in-risk-management) (Health IT Security)

--[Scanners to be patched after government warns of vulnerabilities](https://nakedsecurity.sophos.com/2017/08/09/scanners-to-be-patched-after-government-warns-of-vulnerabilities/) (Naked Security)

--[Five things you need to know about executive protection](http://www.csoonline.com/article/2112401/business-continuity/infosec-staffing-the-six-things-you-need-to-know-about-executive-protection.html) (CSO)

--[Contract obligations, third parties and cyber insurance](http://www.csoonline.com/article/3199686/leadership-management/contract-obligations-third-parties-and-cyber-insurance.html) (CSO)

--[What's the ROI on attribute-based access control?](http://www.csoonline.com/article/3211440/security/whats-the-roi-on-attribute-based-access-control.html) (CSO)

--[OCR’s 'wall of shame' just cracked 2,000 data breaches.](http://seclists.org/dataloss/2017/q3/142) (SecLists)

--[Beware of Security by Press Release](https://krebsonsecurity.com/2017/08/beware-of-security-by-press-release/) (krebs)

--[Russia-linked hackers targeted hotel guests across Europe: security firm](https://www.reuters.com/article/us-cyber-hotels-idUSKBN1AR1IZ) (Reuters)

--[HBO offered $250,000 to hackers in bid to delay data release](https://www.reuters.com/article/us-cyber-hbo-idUSKBN1AR16M) (Reuters)

--[Greater China cyber insurance demand to soar after WannaCry attack: AIG](https://www.reuters.com/article/us-aig-china-cyber-idUSKBN1AP12E) (Reuters)

--[Medical Device cybersecurity is the top challenge to the IOT ecosystem](https://healthitsecurity.com/news/medical-device-cybersecurity-top-challenge-to-iot-ecosystem) (Health IT Security)

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



Contact us: follow @NHISAC and email at [bflatgard@nhisac.org](mailto:bflatgard@nhisac.org)