


# Silos of Excellence

---

 [pylos.co/2020/05/28/silos-of-excellence/](https://pylos.co/2020/05/28/silos-of-excellence/)

Joe

05/28/2020



A new Twitter account appeared on 27 May 2020 for “[NSA Cyber](#)”, claiming the following:

“Welcome to the intersection of threat intel, vulnerability analysis, and technical expertise! All to better equip you against malicious #cyber activity.”

This was a very interesting development, and a separate effort from the US National Security Agency/Central Security Service (NSA/CSS) “official” or main [Twitter account](#). Designed as an outlet specific for the NSA’s relatively new [Cybersecurity Directorate](#), the account quickly proved its bona fides by posting and linking to an NSA/CSS notification on [ongoing Sandworm activity](#) less than a day later.



While interesting on its own for multiple reasons – adding further attribution fuel to the Sandworm discussion and shedding light on ongoing activity by a particularly nasty actor – this is not the first time the Cybersecurity Directorate has directly notified the public of events. Yet such actions stir confusion and add to an overall incoherence in US government cybersecurity policy and activity.

NSA/CSS is a US Department of Defense (DOD) entity and the largest component of the US Intelligence Community. As such, its mission focuses on signals intelligence, cryptography, and DOD signals and cyber security. The vast majority of NSA's mission is offensive (or at least espionage-oriented) in nature, making its role for playing a part in security in any network beyond DOD highly contentious and controversial. That NSA/CSS is now utilizing the Cybersecurity Directorate as an external-facing, publicly-communicating cybersecurity arm is very strange – as presumably this already exists.

Created only in 2018, the US Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) would apparently fill the role of being the US government's vector for communicating with private industry given its mission. While CISA is far from perfect, the idea at least finally created a non-military, civilian cybersecurity agency

to serve as the focal point of US government non-military cyber efforts. Given NSA/CSS's primary mission of signals intelligence (part of which includes conducting cyber intrusions), the private sector is justifiably concerned that trusting this agency for defense could come at significant costs. CISA, although junior in age (and potentially expertise), addresses this core issue of trust by separating the role of liaison from military agencies.

Yet in standing up and using the Cybersecurity Directorate in this way, it would seem that NSA specifically (and perhaps DOD in general) are working to undermine CISA's mission and standing as the lead agency responsible for critical infrastructure defense and coordinating responses with US private industry. A healthy interagency relationship would likely involve NSA and DOD communicating with DHS and CISA to share information, with CISA then taking the lead to promulgate advice and notifications to stakeholders. By going direct, NSA implicitly has made the statement that CISA does not own this mission, cannot be trusted to handle or analyze certain types of information (such as the Sandworm notification), and that NSA (and DOD) will play an independent role in these matters.

While we can argue that NSA will likely retain a capability and talent advantage over any DHS (or even other DOD) elements for the foreseeable future, legitimate questions of trust and primary mission focus mean NSA will never take a lead role in coordinating cyber defense with private industry. Although imperfect, CISA at least represents a move in the proper direction to create a single point of access (and communication) for US government cybersecurity capability and concerns to the private sector.

NSA's use of the Cybersecurity Directorate in this fashion of public communication and defense advisory undercuts CISA's mission and continues the overall incoherence of US cyber policy and cyber defense. For those who have previously worked in the US government, such activity is not surprising as cyber remains "sexy" – and a continued item of significance, which means a source of funding and prestige. Thus a scramble has ensued where various elements of the overall US government – DOD, DHS, the Department of Energy, the Department of Commerce (hello National Institute of Standards and Technology!), the Department of Justice, etc. – all attempt to "own" some aspect of the cyber mission.

Interagency scrambles are especially nasty in the realm of government and private network defense. NSA, US Cyber Command, the Federal Bureau of Investigation (FBI), the Department of Energy (for electric and oil and gas activity), DHS, and CISA all have some stake in this matter, and some wish to own and direct this mission exclusively. The result is a mess where an entity with a question, concern, or an incident doesn't know who to contact – CISA, their local FBI field office, DOE's office of Cybersecurity, Energy Security, and Emergency Response (CESER), or some other organization.

The muddled ownership of the US government role in communicating with or assisting the private sector creates various problems. From lack of clarity in communication, uncertainty in identifying relevant areas of expertise, to "playing one entity against another" tactics where

organizations “shop around” until finding the agency most cooperative all add friction and distraction to the overall defensive mission. Ultimately, the US government has a vested interest in the security of private organizations representing critical infrastructure or national value (such as intellectual property). That decades into the information age the US government is still schizophrenic in its approach to the issue is sad and self-defeating. CISA was (and still could be) a good idea – allowing other entities to basically go rogue and act independently undercuts an agency that is barely two years old, and will create more problems than it may solve.