# White House Announces New Cybersecurity Center

Posted At : February 17, 2015 10:43 AM | Posted By : John Slye

Related Categories: Critical Infrastructure Protection, Intelligence Community, Information Security, Cybersecurity

The White House has announced that it is launching a new federal organization to step up the national cybersecurity coordination and response capability. Details are still slim, but a senior cybersecurity adviser at the White House did outline the vision for the new center in a recent address.

News of the new cyber agency launch hit news sources like **Washington Post** and **Reuters** shortly before the official statement. In the public **announcement**, Lisa Monaco, Assistant to the President for Homeland Security and Counterterrorism, said the new **Cyber Threat Intelligence Integration Center (CTIIC)** will reside within **Office of the Director of National Intelligence** and will be patterned after the National Counterterrorism Center (NCTC). "There are structural, organizational, and cultural shifts that were made in our government in the counterterrorism realm that also apply to cyber. We need to develop the same muscle memory in the government response to cyber-threats as we have for terrorist incidents."

### Filling a Void

In the summer of 2014, the White House created a Cyber Response Group (CRG) in response to the growing number of highly-publicized breaches and intrusions to both public and private networks. Modeled on the Counterterrorism Security Group, the CRG convenes multiple agency players and pools knowledge on current threats. It appears that the CTIIC will build upon the CRG's efforts to "quickly consolidate, analyze, and provide assessments on fast moving threats or cyber-attacks."

"Currently, no single government entity is responsible for producing coordinated cyber-threat assessments, ensuring that information is shared rapidly among existing cyber-centers and other elements within our government, and supporting the work of operators and policy makers with timely intelligence about the latest cyber-threats and threat actors. The CTIIC is intended to fill these gaps," Monaco said.

### CTIIC Functions

Monaco said that the new center will serve a similar function for cyber that the NCTC does for terrorism:

- Integrate intelligence for cyber-threats – information sharing is critical
- Provide all-source analysis to policy makers and operators – cross-domain analysis to provide a comprehensive perspective
- Support the work of existing federal cyber-centers, network defenders, and law enforcement communities – coordinated action and response to achieve common goals.

### What the CTIIC Will Not Do

Monaco was quick to stress that the CTIIC will not *collect* intelligence, but rather it will analyze and integrate information already collected under existing federal authorities. Similarly, Monaco said that CTIIC will not perform functions already assigned to other cyber-centers, but is intended to enable them to perform their respective roles more effectively.

### Looking Ahead

In her remarks, Monaco said that the government will need to work in lockstep with the private sector and do its utmost to share cyber-threat intelligence information, not simply let private entities fend for themselves. The latest budget request from the White House for FY 2016 budget has $14 billion allocated to cybersecurity to protect critical infrastructure, government networks, and other systems.

The CTIIC announcement comes just days ahead of a **White House Summit** at Stanford University to discuss cybersecurity and consumer protections.

### Contractor Implications

It is yet unclear what implications the CTIIC will have for federal contractors. There is limited public information about the role of contractor support at the ODNI and related entities within the Intelligence Community. That said, there is likely to be some need for technology infrastructure in setting up any new entity, and if the demand for skill sets exceeds the government's talent pool then they may look to the contractor community for support.

The broader emphasis on cyber-threat information sharing and related cybersecurity provisions in recent National Defense Authorization bills and others will continue to raise the bar for contractor companies to meet federal cyber-requirements. Increasingly, companies are required to provide agencies with increased visibility into their internal security posture – including reporting incidents – as a stipulation to performing federal work. Expect provisions like these to continue to evolve.