STATEMENT FOR THE RECORD

LT. COLONEL DANIEL J. COONEY

ASSISTANT DEPUTY SUPERINTENDENT, OFFICE OF COUNTER TERRORISM

NEW YORK STATE POLICE

STATEMENT BEFORE THE COMMITTEE ON HOMELAND SECURITY, SUBCOMMITTEE ON EMERGENCY PREPAREDNESS, RESPONSE AND COMMUNICATIONS & SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION AND SECURITY TECHNOLOGIES

MAY 24, 2016

Good morning Chairman Donovan, Ranking Member Payne, Chairman Ratcliffe, Ranking Member Richmond, and members of the subcommittees:

My name is Dan Cooney and I am an Assistant Deputy Superintendent with the New York State Police, responsible for overseeing the New York State Intelligence Center, the State's designated fusion center. Thank you for inviting me to speak today about our cyber threat information and intelligence sharing efforts.

The New York State Intelligence Center, or "NYSIC", is managed by the New York State Police and staffed by approximately ninety people representing nearly twenty law enforcement, homeland security agencies at the local, state and federal levels. Since we opened our doors in 2003 as one of the first fusion centers in the nation we have maintained an "all-crimes" approach, with the ultimate goal of preventing criminal and terrorist activity in our State and supporting our partners' ongoing law enforcement investigations. We are primarily responsible for supporting the fifty-seven counties outside New York City, but we work closely with our New York City Police Department colleagues on New York City-based issues.

NYSIC incorporated cyber threat intelligence into its mission in 2014 by creating a Cyber Analysis Unit. The catalyst was two-fold: we recognized the need to dedicate resources to the growing threat of cyber attacks, and we had just co-located with the Center for Internet Security and the Multi-State Information Sharing and Analysis Center (MS-ISAC), which the U.S. Department of Homeland Security has designated as the cybersecurity information sharing and analysis center for state, local, tribal, and territorial governments. This provided a timely opportunity for us to learn best practices from top cyber security experts. Over time, we were able to staff the unit with an Investigator and four intelligence analysts who possess a mix of specialized technical knowledge or intelligence and analysis experience, a hiring model that has worked well. Our approach is based on partnerships, intelligence production, and outreach, and I will highlight a few examples of the benefits to the State's cybersecurity efforts.

Best Practices in Information Sharing Efforts

The New York State Police has long had a Computer Crimes Unit, and other agencies in New York have worked on cyber threats for some time. We have worked to bolster our relationships with other agencies, not only to learn from them, but to ensure proper information sharing, identify collaborative opportunities and avoid duplication of effort. To that end, the NYSIC

spearheaded the creation of the New York State Cyber Partners Working Group. This group of state and federal government agencies – including law enforcement, homeland security, information technology and the National Guard, to name a few – formally meets on a monthly basis to review cyber threat intelligence and discuss training, exercise and joint project opportunities. As the intelligence center, our role is to take the lead in developing cyber intelligence products for both technical and non-technical audiences, and we leverage the partnerships formed through this group to develop and share intelligence. The Cyber Partners Working Group also joins together for training and exercises. NYSIC, along with its working group partners, has participated in table-top and national level full-scale cyber-related exercises, as both observers and participants. Examples include GridEx III, Cyberstorm V, and New York agency-specific tabletops.

Effective state and federal collaboration is also vital to confronting these challenges. For example, recently NYSIC and its state and federal partners collaborated on the production and dissemination of a joint cyber intelligence bulletin detailing the analyses of detected malware. During the analysis, which determined the malware was a well-documented downloader and credential stealing Trojan, an encrypted file was discovered. Encryption often prevents further investigation; however in this case the team obtained a tool from a partner agency that allowed us to decrypt the file. The file revealed specific and actionable data that could protect IT assets. The NYSIC published these findings as a joint cyber intelligence bulletin and received positive feedback from recipients.

The NYSIC also relies on national cyber information sharing networks. Routinely, we access the National Fusion Center Association's Cyber Intelligence Network (CIN), which is a relatively new network of fusion center cyber analysts, to ascertain whether the intelligence we are developing in New York may be part of a broader trend. The CIN is comprised of over 250 federal, state and local law enforcement members who focus on cyber crimes. These members come together and act as a Virtual Fusion Center utilizing a cloud service provided by the Homeland Security Information Network (HSIN) to share real time cyber threat intelligence in support of an incident, event or mission. This level of cyber threat information sharing was impossible only a few years ago, yet now is becoming routine.

There are several instances in which the CIN collaborated during high-profile events to great effect. For example, the CIN launched the HSIN's secure, web-conferencing platform, called CINAWARE, in response to Distributed Denial of Service (DDoS) attacks launched by cyber hacktivists against several state and local government networks which included law enforcement and emergency medical service entities that were responding to an incident. The CIN immediately began sharing real time intelligence on the attacks with the relevant local agencies. The National Fusion Center Association reports that more than 350 individuals from fusion centers and other federal, state and local agencies around the country participated in the CINAWARE room over a period of several weeks, with an average of fifty to ninety users in the room at any given time. The room was supported 24/7, which included overnight support from the MS-ISAC. During that period, more than 250 queries were submitted and answered via the CINAWARWE room, enabling rapid sharing of information with decision makers. Leaders in state, local, and federal agencies were consistently briefed on the information from the CINAWARE room.

Since that event, the CINAWARE room on HSIN has been opened to support the response to the Vikingdom DDoS attacks against state and local networks across the country, the sharing of cyber specific information related to the Paris Bombings, and to support the law enforcement and homeland security mission for Super Bowl 50. The CIN also facilitates daily sharing throughout the

country of indicators of system-compromise identified in discrete geographic regions, issues and responds to Requests for Information, and acts as a team of subject matter experts to support local operations. All of this sharing occurs between fusion centers utilizing the federal platform, HSIN, and occurs at the For Official Use Only (FOUO) level.

Similarly, the NYSIC's co-location with the Center for Internet Security and the MS-ISAC allows our staff to walk downstairs and talk with their intelligence or operations analysts about nationwide reporting and how it may impact New York State. Any relevant, sharable information these networks provide NYSIC ultimately benefits our Cyber Partners Working Group and the State's broader cybersecurity prevention efforts.

This intelligence is of limited use, however, if we cannot provide it to consumers and decision-makers. Equally as important is communication with those outside of NYSIC. The NYSIC team is constantly meeting and briefing local governments and private critical infrastructure sectors on cyber security concerns. Participants leave with contact information needed to build distribution lists for intelligence products. Our distribution lists are separated by sector, and between technical and non-technical audiences, to ensure recipients receive exactly the information they need. We provide IT staff with actionable intelligence that can be cross-referenced with traffic on their networks, so they can deploy appropriate prevention or mitigation controls. Other partners, such as executives, appreciate more strategic information on trends in cyber actors' tactics, techniques and procedures relevant to their sectors that can help inform better policy decisions. We listen to their feedback and tailor our intelligence products appropriately.

The NYSIC Cyber Analysis Unit may receive or develop intelligence that is particularly relevant to the first responder community, or a subset thereof. For the Fire/EMS/Emergency Management agencies in New York, our team leverages NYSIC's Intelligence Liaison Officer (ILO) network – points of contact in each county from those three disciplines that participate in two-way sharing of threat information with our center. We educate them on cyber threat reporting and the types of technical and analytical support NYSIC can provide. For example, we crafted a cyber bulletin distributed specifically to 911 call centers with an "E-911" capability based on our receipt of threat and vulnerability information relevant to technology that is employed.

Information specific to law enforcement is pushed to agencies in the field using another outreach program called the Field Intelligence Officer (FIO) program. In support of this program, nearly all of the more than 500 law enforcement agencies in New York has a designated FIO that regularly communicates with the NYSIC to advance the homeland security and counter-terrorism mission. We utilize these members to share cyber information in their jurisdictions as well. More technical products, which may include vulnerability and consequence information, are shared directly with county Chief Information Security Officers (CISOs).

New York State is currently working to expand its information sharing with the healthcare sector – both public-and privately-owned facilities. The NYSIC is finding that this sector is willing to partner with the State to discuss intelligence requirements, information sharing, training opportunities and best practices in mitigating cyber threats.

Recommendations for Continued Growth in Information Sharing

New York State has made significant strides in building its cybersecurity capabilities, both at the fusion center and across state agencies. We are sharing more information more effectively than ever before. Policies and best practices have been developed by consensus through multilateral and

interagency policy bodies and professional associations. They are reinforced through daily engagements between federal, state, local, and private sector partners. Despite a constantly changing environment we have made excellent progress.

In order to build upon our successful efforts, we have identified four areas for continued growth.

First, information sharing regarding cyber threats between the federal government and the states should be further streamlined. The information sharing lessons of the last thirteen years in the counter-terrorism space must be applied in the cyber security today. In 2003, as the first New York State fusion center director, I remember working through information sharing issues with DHS, FBI and others. Ultimately, an agreed upon vertical information sharing pathway was developed between federal partners and the fusion centers. At the State level, the fusion center is DHS's single point of contact for terrorism-related information, and we know from which subset of DHS to expect information. This is not yet the case with cyber threat information. There are many entities within DHS that gather, analyze and disseminate various types of cyber threat intelligence, whether it's tactical indicators of compromise, strategic intelligence assessments, or organizing outreach campaigns with private sector entities in our jurisdiction. Given this information – whether it is raw information or finished intelligence – does not come together in one place at the federal level with a designated unit to ensure rapid communication with the fusion centers, more often than not the centers do not receive information in a timely manner. This problem is exacerbated by the fact that other federal agencies also have a cyber mission, and many have not yet built relationships with the fusion centers like DHS or FBI have over the last 13 years. This includes sector-specific agencies like Energy, Treasury, and Health and Human Services that play an important role in protecting key sectors of the nation's critical infrastructure and economy, and who conduct outreach and information dissemination campaigns with private sector entities under their jurisdiction. Any steps that DHS can take to streamline the overall federal cyber intelligence sharing processes with the fusion centers will help states and our local partners better understand the current threat landscape and more efficiently align our own cyber information sharing with the private sector. Working together will better enable us to protect against and respond to inevitable cyber attacks. The more cyber threat intelligence that fusion centers receive, the more we can share with agencies and businesses in our jurisdictions. This will close intelligence gaps and help us communicate threats to smaller entities that federal information sharing currently does not reach.

Second, we must also continue to evaluate how we share classified cyber threat intelligence from the federal government to the fusion centers. There is no central federal system that stores indicators of compromise against which fusion center cyber analysts can run comparisons and lookups. The National Network of Fusion Centers does not have a space on the National Cybersecurity and Communications Integration Center (NCCIC) floor, and therefore lacks access to that critical data source which is available to other federal information sharing partners. The network has interactions at the DHS Office of Intelligence and Analysis' Cyber Intelligence and Analysis Division (CIAD), but that interaction primarily occurs at the FOUO level and involves information being shared up to the federal level, but not necessarily back down. Additionally, we observe that a large amount of cyber threat information is classified. While the NYSIC understands why that might be the case, the federal community needs to continue to focus on creating unclassified tear lines of actionable intelligence. The fusion centers may have the capability to receive classified documents, but cannot share useful contents with many of its customers unless the classification is downgraded. We would be pleased to work with authors of classified documents to develop unclassified actionable information for our non-cleared partners. I believe there has been

some effort to share more unclassified indicators based on recent production efforts by one federal agency, and I hope that effort continues across the federal community.

Third, we need to continue our efforts to share information with local and county governments and private sector. We need to make sure there is consistency, and not confusion, regarding "who to call" when a local government or private entity experiences a cyber incident. We successfully worked through similar issues in the counter-terrorism area and I believe collective development of clear guidance would better serve our customers.

Finally, the parallels between counter-terrorism and cyber extend beyond information sharing. Adequate cyber preparedness requires widespread implementation of best practices and mitigation efforts, which invariably can exceed the capacity of local and county governments facing a growing myriad of threats. In our ever-more connected world, your network is only as strong as its weakest interconnection, yet implementing strong cybersecurity solutions is often costly. As we continue the hard work of policy development and adoption of best practices, the need for federal government support of state and local cybersecurity preparedness should not be overlooked. Much the same way the DHS Homeland Security Grant Program provides essential federal support for counter-terrorism initiatives, similar support for cyber security would further enhance the capacity of states, fusion centers and local governments to prevent and respond to cyber incidents that threaten our nation's critical infrastructure and economy.

Thank you for this opportunity to speak before your Subcommittees. On behalf of New York's fusion center, and as part of the larger National Network of Fusion Centers, I appreciate the invitation to participate in this discussion and I welcome any questions you may have.