

To: Members of the Justice Appropriations Subcommittee
From: Alice Fulk Wisner, LSA
Subject: DPS Follow up on Cyber Crime Unit
Date: February 5, 2016

This answer was provided by the Department of Public Service regarding a question posed during the 1/26/16 appropriations subcommittee meeting: What is the projection of the needs of the DPS and DCI's Cyber Crime Unit (CCU) in the next 3 to 5 years as it relates to cyber-related crimes, attacks, and intrusions?

The number of cyber-related cases received by the DCI's CCU will undoubtedly continue to increase as the number of online transactions and communications increases by the minute. The cases that have been handled by the DCI's CCU have increased exponentially from 2008 to 2015. This increase reflects the amount of users on the Internet and different applications that can be accessed from smart phones and tablets. A number of the cyber cases are handled by DCI Special Agents that are also deputized as Federal Task Force Officers (TFO's) with the Omaha FBI Cyber Crime Unit. The DCI Cyber Crime Unit works closely with the FBI as some of these cases rise to a level of federal classification and are not worked at a state level. Our response to these cases many times becomes limited because the number of requests and the limited manpower to follow up on all inquiries. The DCI CCU attempts to assist with every complaint or Iowa citizen that needs assistance with a fraud or illegal solicitation involving a monetary loss; however, the lack of manpower and the sheer number of requests do not make it feasible to address every complaint or issue.

A true comparison of cases over time can be gleaned from our required federal reporting through affiliation with the *Office of Juvenile Justice Delinquency Prevention (OJJDP)* and the *Internet Crimes Against Children (ICAC) Task Force*. In 2008 the average number of CyberTips received by the DCI CCU/ICAC Task Force was approximately 11 per month, in 2015 that number has catapulted to approximately 52 per month. This is an increase of 373% from 2008 to 2015. The overall number of investigations was not captured in 2008 but the data suggests a similar if not a higher increase. The number of forensic examinations in 2008 was approximately 28 per month, in 2015 there were approximately 231 forensic examinations completed per month. This is an increase of 726% from 2008 to 2015. *(The DCI CCU has partnered with local law enforcement affiliates to assist with this increase. The majority of the examinations and investigations rest with the DCI CCU. The average turnaround time for a forensic examination ranges from 10 to 16 months.)*

The DCI Cyber Crime Unit/ICAC Task Force is comprised of nine (9) sworn members and one (1) civilian criminal intelligence analyst. The breakdown is as follows:

- 1 - Special Agent in Charge (supervisor, ICAC Commander that oversees the local law enforcement affiliates as well)
- 3 – Special Agent Investigators (dividing Iowa into 3 regions)

- 5 - Special Agent Forensic Computer Examiners
- 1 – Criminal Intelligence Analyst

*With the dramatic increase in requests for examinations and investigations since 2008 the DCI CCU has only increased its manpower by adding one (1) additional special agent forensic computer examiner and one (1) criminal intelligence analyst.

*Please note: The certification process to become a forensic computer examiner takes an average of two years.

The DPS/DCI is also a key partner in the State's Cyber Security Strategy Group as outlined in the Governor's Executive Order #87 on Cyber Security. DPS is working with the Office of Chief Information Officer (OCIO), Iowa Homeland Security and Emergency Management, Iowa National Guard and Iowa Communications Network to develop best strategies to protect and prevent cyber disruptions and prepare a coordinated response plan in the event of a significant cyber event. The Division of Intelligence and Fusion Center (DOI/FC) is also engaged with a number of agencies/organizations, including the FBI, USDHS and MS-ISAC and the National Network of Fusion Centers, to monitor cyber security issues and provide information and warnings to state and local governments and the private sector on cyber security issues and events. DPS is currently leveraging its relationship with OCIO for expertise in this area but does recognize the need for a specially trained cyber analyst to be embedded in the DOI/FC for maximum benefit on cyber issues effecting both government and the private sector.