The Utah Model:

A Path Forward for Investigating and Building Resilience to Cyber Crime

BJA
Bureau of Justice Assistance
U.S. Department of Justice

Police Executive Research Forum

This project was funded by Grant No. 2014-D6-BX-K012 awarded by the Bureau of Justice Assistance as part of an effort to help state, local, and tribal law enforcement better understand and address cyber crime. The Bureau of Justice Assistance is a component of the Department of Justice's Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, the Office for Victims of Crime, and the Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking. Points of view or opinions in this document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice. This grant was awarded in partnership with RAND Corporation, the International Association of Chiefs of Police (IACP), and the Institute for Intergovernmental Research (IIR). For more information on the Law Enforcement Cyber Center and related projects, see: http://www.iacpcybercenter.org.

Future Versions

This document should be viewed as a "living document" and will be periodically updated as new content becomes available. BJA and its partners will continue to address cyber crime as a key issue impacting the country.

Individuals and organizations are invited to share potential content or submit recommendations and comments regarding this document via the Law Enforcement Cyber Center at www.iacpcybercenter.org.

[Page Intentionally Blank]

The Utah Model:

A Path Forward for Investigating and Building Resilience to Cyber Crime

[Page Intentionally Blank]

Table of Contents

[Page Intentionally Blank]

For definitional information about key terms used throughout this document, see the Glossary of Terms on page 58.

The Utah Model

> **"There will be consequences for those who use malicious cyber activity to harm Americans or harm American businesses…. We need to get better at helping our state and local partners deal with the threat, because all manner of crimes that we [at the FBI] don't have the resources and time to get to are appearing for the county sheriffs, the local police departments, the local DAs…. One of the things we're trying to do is work with the Secret Service to offer training to the 17,000 state and local law enforcement organizations in this country, to equip their people to be digitally literate. A ton of work is going on there."[1]**
>
> **—FBI Director James Comey**

As new Internet-based technologies are introduced, cyber crime is growing exponentially, both in the proliferation of crimes and the associated impact on victims—i.e., financial loss, invasion of privacy, and even blackmail. Cyber crimes endanger our national security as well. To respond to this ever-changing threat, national and local police agencies across the globe continue to explore ways to coordinate resources with each other and attack the problem. In the United States, combating cyber crime has traditionally been perceived largely as an FBI responsibility, with less involvement by local police. However, as cyber crime victims increasingly report these crimes to their local police, those agencies are being driven to develop programs and partnerships with federal law enforcement agencies in order to understand the roles they can play to be most helpful in preventing and investigating cyber crime.

To better understand what a successful cyber crime program looks like in practice, the Bureau of Justice Assistance tasked the Police Executive Research Forum (PERF), in conjunction with several other partners,[2] with conducting a case study. The Utah Department of Public Safety (DPS) was chosen because it has built a robust program over the past 4 years that involves conducting cyber crime investigations,

[1] FBI Director James Comey, Address, International Conference on Cyber Security, Fordham University, New York, NY (January 7, 2015). https://www.fbi.gov/news/speeches/addressing-the-cyber-security-threat.

[2] The Law Enforcement Cyber Center (http://www.iacpcybercenter.org/) is a cooperative effort between PERF and the Bureau of Justice Assistance, International Association of Chiefs of Police, RAND Corporation, the Institute for Intergovernmental Research, the National White Collar Crime Center (NW3C), the National Governors Association, the Multi-State Information Sharing & Analysis Center (MS-ISAC), the FBI, DHS, and several subject matter experts from other organizations.

analyzing cyber intelligence, and studying the ramifications of cyber crimes on emergency management and critical infrastructure.

The DPS program is known as the "Utah Model." PERF staff members visited DPS headquarters in the greater Salt Lake City area to conduct interviews and gather details from stakeholders directly involved in implementing and running the program. These stakeholders included agency leaders, cyber investigators, fusion center staff, FBI partners, and emergency management personnel. All stakeholders are part of the Utah State Cyber Intelligence Network (USCIN), which is a "partnership designed to support investigations, increase resiliency, improve situational awareness, and disrupt cyber crime."[3]

This publication describes the challenges DPS faced in creating its program, the promising practices that have emerged, and lessons learned, so that other state and local agencies may understand the issues that are involved in building or enhancing their own cyber crime programs. This case study also provides an overview of the key components of a cyber crime program such as leadership, resources, training, and interagency coordination.

[3] Utah Department of Public Safety, "Establishing a Cyber Crimes Unit," White Paper (September 11, 2014). http://docplayer.net/10626312-Establishing-a-state-cyber-crimes-unit-white-paper.html, at 2.

The Reasons for Creating a Cyber Program

Local Cyber Attacks in Utah

Several cyber attacks on the Utah state government precipitated the creation of DPS's Cyber Crimes Unit and made the problem clear for DPS Commissioner Keith Squires. In 2009, for example, cyber criminals were able to impersonate a public university and electronically diverted $2.5 million from a Utah state account into a private account in Texas.[4] State agencies managed to freeze the account to reduce the losses, but were unable to recover approximately $300,000. Investigators believed the theft was committed by a criminal organization in Texas, but were unable to complete a successful investigation.[5]

In 2012, an attacker affiliated with the hacking group *Anonymous* accessed and exploited personal information about Utah State Senator Karen Mayne. The group stated that its action was in retaliation for a bill Senator Mayne was sponsoring intended to curb vandalism through regulating graffiti tools. The criminal actors reportedly launched a denial-of-service attack on the Salt Lake City Police Department's website at the same time.[6] Also in 2012, international cyber criminals hacked into the Utah Department of Health's Medicaid server and gained access to the personal health information of approximately 780,000 individuals.

These incidents and others inspired DPS to take a more active role in investigating cyber crime. Commissioner Squires looks at attacks on Utah state networks as an indicator of what may be happening in the private sector in order to gauge the explosion of cyber crime. In 2010, Utah's Department of Technology Services (DTS)—the information technology provider responsible for securing Utah state networks—reported approximately 25,000 to 30,000 attacks on the system per day. In 2016, DTS estimated that 100 to 200 million attempted cyber attacks bombarded Utah state networks in one day.[7] Of course, the vast majority of attacks are routinely stopped by firewalls and other protective cyber security measures, and many users have no idea how often cyber criminals are looking for cracks in the system's armor. However, just one successful hacking attempt can create havoc on government networks. While the increase in attempted cyber attacks on Utah systems can be attributed partially to the building of a National Security Agency (NSA) facility in Utah,[8] the increase in volume over the course of his tenure demonstrated to the Commissioner the need for proactive enforcement.

---

[4] Andrew Adams, "Thieves Steal $2.5 Million from State Funds," KSL.com (February 12, 2009). http://www.ksl.com/?nid=148&sid=5575095.
[5] Keith D. Squires, "Cybercrimes Enforcement: A State Perspective," *The Police Chief* (February 2014).
[6] Amy Jol O'Donoghue, "Group hacks into SLCPD website over graffiti bill," KSL.com (January 31, 2012). https://www.ksl.com/?sid=19077893.
[7] Keith D. Squires, "Cybercrimes Enforcement: A State Perspective," *The Police Chief* (February 2014).
[8] Lee Davidson, "Massive Utah cyberattacks—up to 300 million per day—may be aimed at NSA facility," *The Salt Lake Tribune* (February 3, 2015). http://www.sltrib.com/news/2135491-155/massive-utah-cyber-attacks-may-be.

The Overall Philosophy of Cyber Investigations

Concerned about the rise in cyber attacks against the Utah government and its residents, Commissioner Keith Squires sought to enhance cyber crime investigation capabilities in his agency.

One major obstacle to securing funding for the resources and capabilities that are needed to conduct cyber investigations is the misperception that cyber crimes—particularly those involving financial crimes or fraud—are "victimless." This is partially due to the fact that, for decades now, banks have built cyber losses into their business models, thereby absorbing the cost of breaches and fraudulent purchases. This means that individual bank customers who experience a loss are promptly reimbursed by their financial institutions, so they may be less concerned than they would be if they suffered a loss without compensation. In many cases, victims never even file a police report.

However, there is some indication that this dynamic may be changing and that cyber losses will no longer be considered "business as usual." Massive cyber attacks in recent years, such as those involving Sony and the Office of Personnel Management, have brought cyber crime into public view. As debit and credit cards change from "swipe" to "chip" technology, which is more secure, banks may no longer simply assume liability for fraud conducted at point-of-sale machines.[9] As businesses change how they think about computer-enabled fraud and no longer consider it an absorbable cost of doing business, this will likely increase the pressure on investigative agencies to identify perpetrators.

It is important for police executives to understand the true impact of cyber crime on an individual or a business—and to understand that banking institutions do not cover all losses. Small businesses incur significantly higher losses per employee from cyber crime than larger businesses,[10] which can significantly impact their operations and viability. Larger businesses face larger total losses and the threat of substantial harm to their reputation and organization. Individuals who are victims of identity theft or other cyber crime may need years to recover financially, or their financial health may be permanently damaged. Damage to an individual's credit rating can impact many facets of that person's life, including applying for a job or obtaining financial aid. Cyber crime victims also report suffering emotional trauma.[11] Moreover, it is a mistake to think of cyber crime as exclusively financial in nature. Crimes like online harassment, "swatting," "revenge porn," and hacktivism can have profound impacts on victims' emotional and physical well-being.

At a national level, the complexity of this issue has made it difficult for the U.S. government to capture the overall extent of the impact. Many studies have tried to measure the losses from cyber crime. A 2014 study by the Center for Strategic and International Studies estimated that cyber crime cost the global economy approximately $445 billion every year, with $160 billion attributed to losses to individuals from

---

[9] Andrew Cohn, "New Credit Card Chips Shift Liability to Retailers," *Insurance Journal* (December 7, 2015). http://www.insurancejournal.com/news/national/2015/12/07/391102.htm.

[10] Ponemon Institute, "2012 Cost of Cyber Crime Study: United States" (October 2012), at p. 3. https://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf.

[11] Office for Victims of Crime, Expanding Service to Reach Victims of Identity Theft and Financial Fraud (October 2010). http://www.ovc.gov/pubs/ID_theft/pfv.html.

hacking and $150 billion attributed to losses connected to the theft of personal information.[12] Victim complaints filed with the Internet Crime Complaint Center (IC3) in 2014 had an estimated total loss of more than $800 million,[13] and only an estimated 10 percent of all cyber crimes are reported to IC3.[14] The Ponemon Institute estimated in 2015 that the average annual losses to companies worldwide exceed $7.7 million, an increase of 19% from the prior year.[15]

> **"Most cyber crimes are property crimes, so people may think that they're less important than violent crimes. But cyber crimes can be devastating to victims. Police have a fundamental duty to help protect people from cyber criminals."**
>
> ***—Commissioner Keith Squires, Utah Department of Public Safety***

The Utah Department of Public Safety's Cyber Capabilities

In the wake of major cyber attacks in Utah and the commitment to addressing this growing area of criminal behavior, Commissioner Keith Squires created a Cyber Crimes Unit within the Department of Public Safety's State Bureau of Investigation (SBI) in 2012.

Organizationally, the Cyber Crimes Unit is positioned in the SBI Major Crimes Investigations branch. But as part of *Operation Wellspring*—a partnership between IC3, FBI field offices, and state and local law enforcement agencies—the Cyber Crimes Unit is physically housed at the FBI's Salt Lake City Field Office. The Cyber Crimes Unit consists of one full-time sergeant and two full-time detectives. The unit reports to the lieutenant who oversees major crimes investigations and the captain who is responsible for the entire State Bureau of Investigation.

The Cyber Crimes Unit also has two civilian members. A cyber intelligence analyst is housed within the Utah Statewide Information and Analysis Center (SIAC), Utah's designated state fusion center. The cyber intelligence analyst provides subject matter expertise to the cyber crime investigators, and is responsible for cyber intelligence analysis as well as outreach efforts to the private sector for the coordination of

[12] James Lewis, *The Economic Impact of Cybercrime and Cyber Espionage*, Center for Strategic and International Studies (July 2013). https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/60396rpt_cybercrime-cost_0713_ph4_0.pdf.
[13] The Internet Crime Complaint Center, "2014 Internet Crime Report," p. 4. https://pdf.ic3.gov/2014_IC3Report.pdf.
[14] Police Executive Research Forum, "The Role of Local Law Enforcement Agencies in Preventing and Investigating Cybercrime" (2014). http://www.policeforum.org/assets/docs/Critical_Issues_Series_2/the%20role%20of%20local%20law%20enforcement%20agencies%20in%20preventing%20and%20investigating%20cybercrime%202014.pdf.
[15] "Forewarned is Forearmed: 2015 Ponemon Institute Cost of Cyber Crime Study." http://www8.hp.com/us/en/software-solutions/ponemon-cyber-security-report/index.html?jumpid=va_fwvpqe387s.

SIAC's Cyber Intelligence Liaison Officer (ILO) Program. The cyber intelligence analyst provides invaluable assistance to investigators on complicated technological issues, and performs the primary function of vetting cyber case referrals to see if various investigations should be pursued.

The Cyber Crimes Unit also has the assistance of a digital forensic analyst who has been housed at the FBI's Regional Computer Forensics Library (RCFL) since 2012. In addition to performing forensic analyses, this analyst also serves as a resource for investigators on complicated technical issues or when they need additional support. The digital forensic analyst meets regularly with the Cyber Crimes Unit and participates in investigations and training (e.g., tabletop exercises simulating cyber critical incidents).

The Cyber Crimes Unit benefits from a variety of partnerships with other state, federal, and private-sector partners (see figure 1).

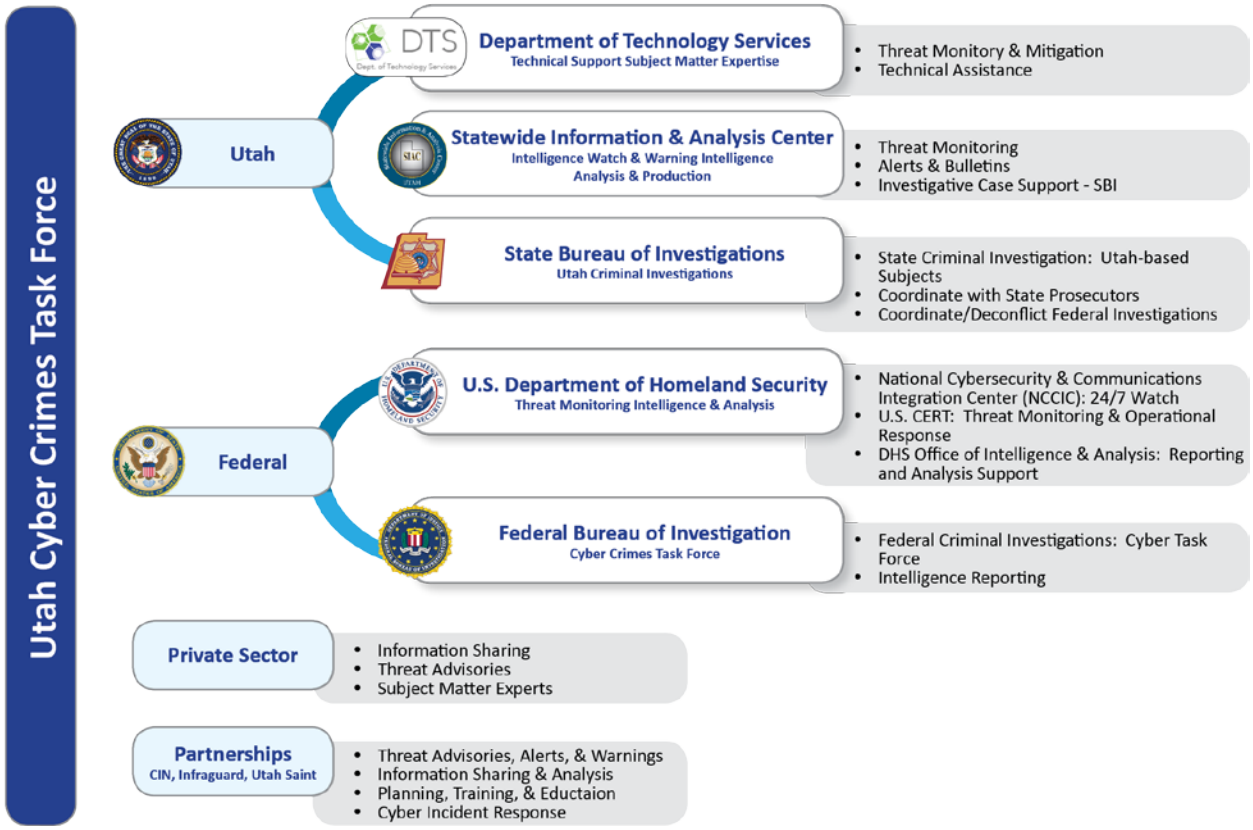


Figure 1: Utah Cyber Crimes Unit[16]

[16] Utah Department of Public Safety, "Establishing a Cyber Crimes Unit," White Paper (September 11, 2014). http://docplayer.net/10626312-Establishing-a-state-cyber-crimes-unit-white-paper.html, at 7.

The Utah State legislature authorized funding for the cyber intelligence analyst and three full-time cyber investigators in 2012. Importantly, this is the only funding with which DPS's Cyber Crimes Unit operates. Despite serving as the pilot site for the FBI's Operation Wellspring, that partnership did not come with federal funding, unlike many other joint state and federal task forces. It is therefore important for police executives who are considering their own cyber partnerships to understand that while there are many benefits to working with the FBI, they may need to secure the funds to staff full-time investigators from their own state resources.

Commissioner Squires selected personnel for the unit who demonstrated technological proficiency or a background in computers. In order to bring the investigators up to speed on advanced technical aspects of cyber crime, Commissioner Squires procured federal funding to send staff members to the U.S. Secret Service's National Forensics Computer Institute in Hoover, Alabama. Investigators also took courses offered by SANS, a private institute specializing in computer security.[17]

Importantly, investigators from Utah are paired with counterparts at the FBI through the course of their investigations. Working together provides the SBI's cyber investigators with opportunities to build skills in the context of active investigations.

Commissioner Squires established Utah's current program in phases. In 2012, DPS stood up its Cyber Crimes Unit with funding from the state legislature. The Commissioner labeled DPS's efforts that year as "trying to find our way in the dark," by trying to understand the problem and seeing what the department could do. The Utah State Department of Technology Services was an influential partner, providing subject matter expertise and technical assistance to investigators. However, the number of cases that the Cyber Crimes Unit could investigate was quite limited. The unit experienced challenges when confronted with cases where the victims or perpetrators were located outside of Utah, which is common in the realm of cyber crime. Without a national or international reach, the unit could not really begin to make a significant impact on the cyber crime problem in Utah.

To address this challenge, Commissioner Squires joined with a group of state and local police executives to seek federal assistance on cases in Utah, and also create a network of individuals concerned about the problem on a national level, similar to nationwide High Intensity Drug Trafficking Area (HIDTA) initiatives.[18]

Commissioner Squires went on a tour of the FBI's IC3 facility during this time and credits that with "opening his eyes." During the visit, IC3 staff gave Squires a sample cyber crime "packet" (see IC3 sidebar, next page)—a file of information about a particular case regarding the crime, suspect, and potential victims.

Squires then began discussions about creating a dedicated, state-level cyber crime program with the FBI, based on an assessment of the capabilities and resources of the group's members. The FBI then partnered

[17] For a list of government-sponsored trainings available for investigators, see the Law Enforcement Cyber Center's Training page at http://www.iacpcybercenter.org/topics/training-2/.
[18] Utah Department of Public Safety, "Establishing a Cyber Crimes Unit," White Paper (September 11, 2014). http://docplayer.net/10626312-Establishing-a-state-cyber-crimes-unit-white-paper.html.

with DPS to establish the first pilot program, called "Operation Wellspring," in 2013. Wellspring is an effort to join state and local officials on a task force to address high-tech crime and computer-enabled crime, particularly cases referred from IC3. Following the initial pilot, the FBI declared Operation Wellspring a success, and, as of November 2016, has implemented the Wellspring Model in nine other regions throughout the United States—San Diego, New York, Buffalo, Knoxville, Oklahoma City, Phoenix, Albany, New Orleans, and Kansas City, Missouri.

The Internet Crime Complaint Center

The Internet Crime Complaint Center (IC3) is the FBI's clearinghouse for receiving cyber crime complaints from the public. Its mission is to provide the public with a "reliable and convenient reporting mechanism to submit information to the Federal Bureau of Investigation concerning suspect Internet-facilitated criminal activity and to develop effective alliances with law enforcement and industry partners."[19] The FBI established IC3 in 2000, initially to look at Internet fraud, and later expanded its purview to a comprehensive list of Internet crimes.

There are enormous challenges with building a dataset that captures all cyber crimes throughout the United States. For example, in 2015, IC3 received over 8,000 business email compromise and email account compromise complaints that related to the combined loss of almost $275 million.[20] But Joseph Demarest, Associate Executive Assistant Director for the FBI's Criminal, Cyber, Response, and Services Branch, has estimated that only about 10 percent of all cyber incidents are reported to IC3.[21]

Partnerships between IC3 and state and local agencies are putting IC3's database of complaints into action. IC3 makes its database of complaints available to all sworn police officers through the FBI's Law Enforcement Enterprise Portal (LEEP), and allows officers to aggregate victims and losses within their jurisdiction. For example, if the individual monetary losses associated with a cybercrime are too small to justify an investigation but investigators later discover that the same perpetrator committed multiple minor offenses, detectives are able to identify and reopen these types of cases. IC3 also issues intelligence that state and local police agencies can use to inform investigations, including public service announcements, scam alerts, and intelligence products that describe emerging threats.

[19] https://www.ic3.gov/about/default.aspx.
[20] Federal Bureau of Investigation, The Internet Crime Complaint Center, 2015 Internet Crime Report (2015). https://pdf.ic3.gov/2015_IC3Report.pdf.
[21] Police Executive Research Forum, "The Role of Local Law Enforcement Agencies in Preventing and Investigating Cybercrime" (2014), p. 1. http://www.policeforum.org/assets/docs/Critical_Issues_Series_2/the%20role%20of%20local%20law%20enforcement%20agencies%20in%20preventing%20and%20investigating%20cybercrime%202014.pdf.

Participation in Operation Wellspring specifically allows state and local law enforcement agencies to receive case referrals in the form of IC3 "incident packets," which are packaged to contain all available information. IC3 puts special emphasis on cases that do not meet most federal investigative thresholds, but which local agencies might investigate. In 2015, the IC3 provided 165 referrals to the 8 Operation Wellspring sites, which then opened 39 investigations that involved approximately 3,650 individual complaints and financial losses totaling approximately $55 million.[22]

As Utah DPS's cyber capabilities continue to grow, Commissioner Squires is placing special emphasis on expanding two areas. First, the Commissioner is bringing the private sector into the Utah Statewide Cyber Intelligence Network (USCIN). Recruiting partners from academia, the financial sector, critical infrastructure, and other private industries is essential, he feels, to developing a proper understanding of cyber threats in the state of Utah. DPS is currently pursuing a significant outreach effort to allow private-sector partners to receive or share information on cyber threats at a level that they feel comfortable with (for more information, see the section "*Promising Practice: Build State Information Sharing Initiatives that Allow Private-Sector Partners to Dictate the Terms of Their Involvement*").

Second, the Commissioner is integrating cyber response planning into the state's existing homeland security apparatus. Because of the potential for cyber attacks to damage critical infrastructure and disturb public safety, it is crucial for state agencies to recognize cyber attacks and develop proper incident response plans in the event of a cyber attack. The Commissioner tasked emergency management officials in the state (the Utah Department of Emergency Management) to integrate a Cyber Incident Response Plan into the state's Emergency Operations Plan (EOP) and Continuing of Operations Plan (COOP). Officials in Utah are now undergoing simulated tabletop exercises to test these plans and train personnel.

Police Departments Are Also Victims of Cyber Crimes

Law enforcement agencies increasingly are becoming the victims of cyber crimes themselves. Government entities are attractive cyber targets because of the sensitive information they guard and the political nature of many cyber crimes. Some of the recent trends that have affected police departments and government officials are described below.

Hacktivism and Doxing

Hacktivism involves breaking into a computer system for the purpose of drawing attention to a social or political cause. Often, many of the perpetrators are juveniles who typically aim to either extract personally

[22] Federal Bureau of Investigation, The Internet Crime Complaint Center, 2015 Internet Crime Report (2015). https://pdf.ic3.gov/2015_IC3Report.pdf.

identifiable information (PII) about police personnel or make a police department's website unavailable to the public through a denial-of-service attack (DoS).

Police departments across the United States have been experiencing a rise in hacktivism targeting their networks.[23] For example, the chief of the St. Louis County Police Department received a threatening message from the hacker group *Anonymous* following the fatal shooting of Michael Brown by a Ferguson, Missouri, police officer in August 2014. The message stated that if the police chief refused to release the name of the officer involved in the Brown shooting, the chief's daughter's personally identifiable information would be released.[24] The group later misidentified an officer it claimed was responsible for shooting Michael Brown. The group did not follow through on the threat to the police chief, but many officers responding to civil unrest in Ferguson were "doxed," meaning their home addresses, Social Security numbers, and phone numbers were made public.

In another particularly alarming cyber attack on police, the ISIS-affiliated Caliphate Cyber Army disclosed PII of 36 Minnesota police officers. The ISIS group called for the officers to be killed, and it was considered "a serious threat" by the FBI's Minneapolis Field Office.[25]

A September 2016 guide published by the Bureau of Justice Assistance and the Criminal Intelligence Coordinating Council underscores the increasing need for police officers and their families to protect themselves online. Police personnel can take relatively simple steps, such as strengthening their social media privacy settings and protecting their home Wi-Fi network through encryption, to proactively mitigate cyber threats.[26] While these practices are advised for all Internet users, police personnel have a particular need to remain up-to-date to protect their facilities from the latest malicious technology and digital threats.

Ransomware

Police departments, hospitals, and local government agencies have also increasingly been the victims of ransomware attacks. Ransomware is a type of malicious software—often introduced to a network through phishing—that locks files until users pay a ransom (typically in the form of anonymous virtual currencies such as Bitcoin). In some cases, files are encrypted until a ransom is paid, which is known as "crypto-ransomware."

---

[23] Aaron Boyd, "Alert: Public officials at increased risk of hacktivist attacks," *Federal Times* (April 23, 2015). http://www.federaltimes.com/story/government/cybersecurity/2015/04/23/alert-public-officials-hacktivist-attacks/26241497/.

[24] Alex Rogers, "What Anonymous Is Doing in Ferguson," *TIME* (August 21, 2014). http://time.com/3148925/ferguson-michael-brown-anonymous/.

[25] Libor Jany, "Local Authorities, Feds Investigating Alleged ISIL 'kill List' for Minnesota Law Enforcement," *Star Tribune*, Star Tribune Media Company LLC (March 15, 2016). http://www.startribune.com/fbi-investigating-alleged-isil-kill-list-for-minnesota-law-enforcement/372138411/.

[26] Criminal Intelligence Coordinating Council, Understanding Digital Footprints: Steps to Protect Personal Information; A Guide for Law Enforcement, Bureau of Justice Assistance (September 15, 2016). https://www.it.ojp.gov/GIST/1191/Understanding-Digital-Footprints--Steps-to-Protect-Personal-Information.

Some ransomware attacks are sophisticated, with dramatic countdown warnings, instructions for purchasing Bitcoin, and criminal technical support contact information.[27] Government agencies, such as the Multi-State Information Sharing & Analysis Center (MS-ISAC) [28] and FBI, have warned about increases in ransomware infections and found that exploiting network vulnerabilities and holding digital files hostage is a billion-dollar industry. In 2014, cyber experts estimated the use of crypto-ransomware grew by 114 percent.[29] Some ransomware now threatens to publish the targets' files online unless they pay,[30] which can be problematic for police agencies that manage sensitive information about crime victims and active investigations.

Police departments are especially vulnerable to ransomware attacks because they often lack funding for network security and must rely on outdated technology. Although the FBI advises against paying ransoms, several police departments have chosen to pay these ransoms.[31] Further, police leaders fear that cyber criminals hacking their networks have the potential to compromise evidence in criminal prosecutions.

Swatting

Police departments increasingly are using cyber investigators to target the perpetrators of "swatting" incidents. Swatting incidents involve a fake report of an emergency such as an active shooting incident or home invasion that cause local police departments to send in a SWAT response team. Such incidents not only waste police resources, they can be very dangerous, because the police respond to what has been reported as a high risk situation, but the homeowner did not make the fake emergency call and has no idea what is happening. In the confusion, people can get hurt.

Although crimes like filing a false police report and calling in a bomb threat are not new, their tenor has changed dramatically in recent years. Swatters can "spoof" their phone number or IP address in order to misrepresent or conceal their identity, or have it appear to police as if a call is coming from the victim. Many swatters are experienced criminals who may be involved in other crimes like identity theft or stolen credit cards. Criminals can also visit the dark web to request a proxy individual to perform the swatting for them, sometimes even purchasing prebuilt swatting malware that simply requires the click of a

[27] Chris Francescani, "Ransomware Hacks Blackmail U.S. Police Departments," NBC News (April 16, 2016). http://www.nbcnews.com/news/us-news/ransomware-hackers-blackmail-u-s-police-departments-n561746.
[28] Center for Internet Security Primer: Ransomware Recommendations, Center for Internet Security (September 2014). https://msisac.cisecurity.org/whitepaper/documents/SecurityPrimer-Ransomware.pdf.
[29] Symantec, *2014 Internet Security Threat Report* (April 2014), p 7. http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf.
[30] Symantec, *2016 Internet Security Threat Report* (April 2016).
[31] Chris Francescani, Ransomware Hacks Blackmail U.S. Police Departments, NBC News (April 16, 2016). http://www.nbcnews.com/news/us-news/ransomware-hackers-blackmail-u-s-police-departments-n561746.

button.[32] Swatting can also be a way to show off, prank, or exact revenge. Police have also expressed concern about the potential for swatters to use the tactic to harass women and girls in cyberspace.[33]

Swatting diverts emergency service units from real emergency calls, which can have a large financial impact on departments that deploy specialty resources. Swatting also risks the lives of officers and unsuspecting swatting victims. In Sentinel, Oklahoma, for example, the chief of police was shot four times when he responded to a report of a bomb threat. The homeowner had not made the call and reportedly shot the chief because he did not know that it was police entering his home.[34] Police officers, prosecutors, and others involved in the criminal justice system are increasingly becoming targets themselves of swatting calls when working on high profile cases.

Handling Suspected Swatting Hoaxes

What should the police response be to a suspected swatting hoax? Although police departments must investigate all alleged reports of emergency situations, SWAT teams can approach the scene of a suspected swatting hoax already aware of the dynamics at the scene. Some police departments are training all personnel in the signs of swatting and developing protocols for getting that information to SWAT teams. Training is sometimes provided department wide—not only to 911 call-takers—because many swatting calls come to local police stations rather than 911.

[32] David Costantino, "Swatting, Doxing, and PEDs: Investigative Strategies and Best Practices," Massachusetts Attorney General's National Cyber Crime Conference, April 4, 2016, Four Points by Sheraton, Norwood, MA.
[33] Jason Fagone, "The Serial Swatter," *The New York Times* (November 24, 2015). Where a teenager heavily involved in online gaming threatened to dox and swat female players if they refuse to speak with him. http://www.nytimes.com/2015/11/29/magazine/the-serial-swatter.html?_r=0.
[34] Raph Ellis, "No charges after Oklahoma police chief shot four times," CNN (January 18, 2015). http://www.cnn.com/2015/01/17/us/oklahoma-police-chief/.

Defining the Scope of a Cyber Program

Defining "Cyber Crime"

General Considerations

There is no single definition of "cyber crime" in the United States, leaving agencies to define the offenses for themselves. The result is a wide array of definitions, both exceptionally broad and particularly narrow. This is problematic, because agencies lack common standards for cyber investigations.

Some agencies have adopted a conservative understanding, defining cyber crime only as attacks against computers, networks, and the information and data held within those systems. This limits cyber crime to offenses like network intrusion, infecting systems with malware, and distributed denial of service (DDoS) where multiple systems are coordinating an attack to make a target's website inaccessible. Even if an attacker does not financially benefit from the attack, the intrusion or disruption itself can be criminal.

Other agencies choose a more inclusive approach, considering any crime that is computer-enabled to be a cyber offense. This could include traditional crimes that are carried out with the assistance of technology such as fraud, theft, and narcotic sales.

Europol's Organized Crime Threat Assessment considers "Internet technology…as a key facilitator for the vast majority of offline [organized] crime activity,"[35] but the use of technology in the commission of a crime is also commonplace among more petty criminals.

Some agencies employ an even wider definition, considering a crime to have a cyber element if any type of digital evidence is used in an investigation. Agencies may also consider themselves cyber investigators if they participate in task forces related to Internet crimes against children.

Agencies attempting to define cyber crime must also take into consideration the identity and motives of cyber criminals. In today's world, any traditional criminal could theoretically be a cyber criminal. While organized crime groups, state actors, and terrorist entities have significant resources to commit cyber offenses, any individual with an Internet-connected device is able to inflict significant harm upon unsuspecting victims. Cyber crime can span the spectrum of severity, from major state-sponsored intrusions into critical infrastructure to individual instances of identity theft.

[35] Europol, *EU Internet Organized Threat Assessment*: iOCTA 2011, File No. 2530-274 (April 28, 2011), p. 6.

Changes in technology have "created a new, darker methodology for crimes to be committed by anyone with a computer, a cellphone or smartphone, a connection to the Internet, and a bit of technical expertise."

—Tracey Trautman, Acting Director, Bureau of Justice Assistance

As the world becomes more interconnected and further attached to the "Internet of things," crimes like fraud, child exploitation, and terrorism are rapidly expanding. Despite the lack of consensus on defining cyber crime, local jurisdictions are reporting that almost all crimes they investigate have a cyber component.[36] Even so, many criminal defendants are still prosecuted under "traditional" criminal laws due to the lack of comprehensive legislation regarding computer crimes.[37] Cyber crime, in all its forms, will continue to grow as technology becomes more prevalent and advanced, increasingly blurring the line between cyber crime and "real world" crime.

What Is Cyber Crime?

- "High-tech" or "Computer-directed" crimes: Attacks against computers or networks such as network intrusion, malware investigations, distributed denial of service (DDoS)
- "Computer-enabled" crime: Traditional crimes that are now committed using computers
- Crimes with a cyber component: Any crime where digital evidence is created or collected

Why is employing a clear definition important with regard to cyber crime? Some law enforcement agencies argue there is a need to distinguish between high-tech crime and computer-enabled crime so that investigators can specialize. For example, because network intrusion may require a unique set of skills to investigate, some police executives want investigators who can exclusively dedicate themselves to those types of cases.

At a federal level, it is challenging to build meaningful statistics that capture the frequency and composition of cyber crimes. The Federal Bureau of Investigation uses the Uniform Crime Reports (UCR) and National Incident Based Reporting System (NIBRS) to allow state and local law enforcement to report

[36] Joshua Philipp, "Nearly Every NYC Crime Involves Cyber, Says Manhattan DA," *The Epoch Times* (March 2, 2013). http://www.theepochtimes.com/n3/1476827-nearly-every-nyc-crime-involves-cyber-says-manhattan-da/.
[37] Congressional Research Service, "Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement" (January 15, 2015).

crimes in their jurisdictions to the FBI. Understanding the complication that cyber aspects can bring to classifying crimes, FBI Director James Comey has directed committees of experts to establish a comprehensive method for accurately capturing and accounting for cyber crime. The National Academy of Sciences, for example, recommended that agencies report computer-enabled crimes as traditional crimes with the option to share an attribute of whether computer data or systems were an "integral part of the *modus operandi* of the offense." This change could take place gradually as more local and state agencies transition to more detailed recordkeeping under NIBRS.[38]

Without an accurate picture of the amount of cyber crime in the United States, it can be difficult even for proactive police departments to secure funding to investigate and pursue cyber cases.

[38] National Academies of Sciences, Engineering, and Medicine, *Modernizing Crime Statistics—Report 1: Defining and Classifying Crime.* Washington, DC: The National Academies Press (2016), at 136. https://www.nap.edu/catalog/23492/modernizing-crime-statistics-report-1-defining-and-classifying-crime.

Computers as a Tool versus Computers as a Target

The following examples demonstrate just how important classifying a cyber incident can be:

Example 1a - Not a Question of Cyber Crime: A principal of a local middle school receives a phone call at her office warning that a bomb will detonate at 2 p.m. The caller then hangs up. The perpetrator is not very savvy technologically and believed, incorrectly, that dialing *67 would anonymize the call completely. Local police call the telephone service provider, and, based on the fact that there are exigent circumstances, are able to obtain a precise address for the individual. Is this a cyber crime?

Many observers may not consider this to be a cyber crime, because it does not target a computer or network and did not use the Internet to further the criminal activity. Regardless, many cyber crime units handle such crimes, because detectives are able to quickly retrieve evidence from telephone or Internet service providers.

Example 1b - Both Computer-enabled and Cyber Crime: Next, consider that the middle school principal receives the same phone call. The police officer assigned to work the case reports the threat to the state's fusion center and is informed that 10 other schools in the jurisdiction have reported similar calls that day. After investigation, police officers are able to determine that the threats were made via a robocalling program that uses a computerized autodialer to deliver a prerecorded message en masse through stolen Voice over Internet Protocol (VoIP) accounts (technology that transmits voice calls using Internet Protocol [IP] addresses, enabling users to make telephone calls from any geographic location).

In this instance, the cyber criminal perpetrated both a computer-enabled crime and a cyber crime. The cyber criminal used computer technologies to commit the crime of calling in a false bomb threat, using the Internet to further the criminal activity. The crime started, however, when the cyber criminal stole VoIP accounts—targeting property associated with a computer network—in order to mask his or her identity.

Example 2 – Computer-enabled Crime: An elderly man files a police report upon the advice of the Better Business Bureau (BBB). He describes how he received a telephone call purporting to be from a prominent software company that stated his computer contained viruses and needed to be fixed. The man on the phone charged the man $200, purportedly to remotely manage his desktop and remove the viruses. After several weeks of suffering through constant web browser "pop up" windows, the man decided to report the company for poor service. He then learned from the BBB that he has been a victim of what is commonly known as "tech support scams."

This is a computer-enabled fraud crime that allows cyber criminals to use the Internet and computers to further their underlying fraud.

Example 3 - Both Computer-enabled and Cyber Crime: A hacker compromises the network of a company that offers reverse mortgages. Examining the company's network for several months, the hacker is able to capture a significant amount of personal information (names, addresses, phone numbers) about multiple applicants, which she then sells to a scammer in the dark web. (Note that many cyber crimes start after the large-scale sale or theft of bulk data.) The scammer then calls each number knowing that the individuals who obtain reverse mortgages tend to be elderly, more likely to be less technologically savvy, and more susceptible to a tech support scam. Once the scammer has compromised the victims' desktops, she opens files with titles like

"Important Passwords" and copies the victims' information in order to commit further identity theft.

As these examples demonstrate, the line between computer-directed crime and computer-enabled crime is not always easy to distinguish, particularly at the outset of an investigation. Often, one type of crime in a given case leads to other types of crime.

Lesson Learned: Defining Cyber Crimes Remains a Major Challenge

For Commissioner Squires, defining the scope of DPS's cyber program was the first major challenge to address. The unit's mission does not limit itself to computer-directed crime cases where the computer itself is the target of the crime; it also investigates traditional types of crime that are facilitated by computers. But DPS's cyber program is not all-inclusive; for example, DPS does not task the unit with cases related to Internet crimes against children and other major crime investigations that simply involve digital evidence. The unit focuses its efforts and limited resources on crimes that have a critical mass of its investigations related to the Internet, with either the computer as a target, or the computer as a tool, or both.

DPS may expand and devote specialized investigators to work exclusively on high-tech crimes like DDoS, hacking, and business email compromises and deal with computer-enabled crimes such as online fraud and scams. But these decisions will be heavily influenced by funding and available resources of local Utah agencies to investigate easier cases. At this point, it is important to the Utah legislature and DPS that the state has the capabilities to address the growing volume of financial losses to businesses and individuals in the state from computer-enabled financial crimes.

In explaining the need to address Internet-enabled financial crimes, the Commissioner wanted to provide a solution to fill an obvious gap. The FBI does not have the resources or capability to address all cyber crime and therefore limits its investigations to the most serious cases—often drawing the line at a specific dollar amount as a threshold. So, cyber criminals whose crimes do not meet the FBI threshold often feel as if they can get away with massive amounts of theft and defrauding without any consequences. Commissioner Squires explained that allowing crime to continue in this way, unaddressed by any law enforcement agency, runs antithetical to the values he lays out for his agency. "It was incredibly frustrating to see criminals committing crimes and getting away with it," he said.

Prioritization

Promising Practice: It Is Essential for State and Local Police Agencies to Prioritize Cases and Leads on Potential Cyber Crimes

Cyber crimes are so numerous that there is a fundamental truth in all investigative agencies: the volume and difficulty of the cases make it impossible to address every lead or report. Commissioner Keith Squires said that the key to his philosophy was "recognizing our investigators need to triage."

The Cyber Crimes Unit uses two factors to assess whether to open an investigation. The first inquiry focuses on finding a way to quantify the severity of the crime. While prioritization is crucial, Commissioner Squires did not want the Cyber Crimes Unit to have a specific monetary threshold. So while there is no particular dollar loss required in order to open an investigation, it still is important to focus resources on the worst cases, which will often involve larger financial losses.

A cyber crime involving a small financial loss can be linked with others to assess a cyber criminal's actions in the aggregate. Additionally, there could be a cyber crime that initially causes no financial loss but instead targets the theft of sensitive data like personally identifiable information (PII) or protected health information (PHI). It is not prudent to focus exclusively on monetary losses in these cases, because the stolen data could be monetized much later in the future and then be difficult to link back to any particular breach or data theft.

The second criterion is the quality of the evidence and likelihood of having a successful investigation. Importantly, the end goal of the investigation need not be to effect an arrest. If the quality of evidence leads the Cyber Crimes Unit to uncover good intelligence, disrupt a cyber criminal network, or help prevent a cyber criminal from attacking a Utah business or government agency, for example, then the investigators may open the case. Ultimately, however, investigators must try to avoid wasting their resources on investigations that will lead to a dead end because of the Internet's extreme ability to mask criminal activity.

> **"We're still operating in the Wild West on horses while the criminals are using cars."**
>
> ***—Major Brian Redd, Director, Utah State Bureau of Investigation***

As a result, the success of an investigation often hinges on the lack of sophistication of cyber criminals. A great deal of technology is available today that enables criminals to cover their digital footprints, but cyber criminals make mistakes in not consistently or correctly using this technology. Thus, cyber criminals can often be tracked by the mistakes that they make.

For example, the software application known as "Tor" enables users to conceal their identity and Internet activity from network traffic analysis. And the DPS Cyber Crimes Unit does not currently have the

technology to de-encrypt Tor. However, there are many cyber cases in which criminals did not bother to use Tor, and so DPS gives a higher priority to these cases with accessible evidence.

Tor and Other Anonymity Tools

Cyber criminals today use a wide variety of methods to conceal their online activity. There are many types of technology available to make it difficult to trace a criminal perpetrator's location, from simple services that can spoof a caller ID number to sophisticated software that makes it virtually impossible to locate an IP address. IP addresses are the primary means in cyber crime investigations for locating the physical location of the device where the perpetrator accessed the Internet.

One very popular tool is Tor (The Onion Router). Tor software is freely available and maintained by a nonprofit organization, easily downloadable from the web. It was created to ensure the privacy of users by keeping their activity and communications private and free from monitoring. Tor ensures strong encryption and anonymity by encrypting a user's communication multiple times before connecting to the intended Internet service.[39] Because of these features, Tor is used by many at-risk individuals across the world, including human rights activists, whistleblowers, dissidents, and citizen journalists. But it is also used by cyber criminals. For example, Silk Road, an online marketplace for legal products as well as illegal products—primarily narcotics—used Tor's "hidden services" in order to sell illegal goods, often using Bitcoins.[40]

Garlic routing," embodied in programs like the Invisible Internet Project (I2P), is a variant of onion routing that adds further security to messages. Garlic routers bundle up multiple encrypted messages and therefore make it even more challenging for investigators to perform a traffic analysis of a particular communication.

Another challenge for investigators is cyber criminals' use of Virtual Private Servers (VPS). VPSs are virtual machines that allow private customers to lease server space from an Internet host, often a Bulletproof Hosting Services (BPHS) company.[41] Cyber criminals can rent a server for a low rate to pay for a temporary place to host an attack. Companies that maintain VPSs often do not retain any data, so it is impossible for investigators to know who leased the infrastructure at the time of a particular crime. There are also middle men who purchase blocks of servers and resell them to bad actors.

---

[39] Dune Lawrence, "The Inside Story of Tor, the Best Internet Anonymity Tool the Government Ever Built," *Bloomberg Businessweek* (January 23, 2014). http://www.bloomberg.com/news/articles/2014-01-23/tor-anonymity-software-vs-dot-the-national-security-agency.

[40] *Ibid*.

[41] Max Goncharov, "Criminal Hideouts for Lease: Bulletproof Hosting Services," Trend Micro, Incorporated (2015). http://housecall.trendmicro.com/media/wp/wp-criminal-hideouts-for-lease-en.pdf.

One challenging aspect of cyber investigations for police agencies is managing victims' expectations. Many individuals and businesses do not understand the sophistication with which criminal actors can mask their activity on the Internet. Victims may expect that if they report a cyber crime to a police agency, they will be able to recoup their financial losses or see their offender arrested. Commissioner Squires noted, "One of our issues has been that our existence creates a false expectation. Victims think that if they take the time out of their schedule to report, they will get their money back."

To help manage expectations, DPS ideally could train one of the department's victim advocates to be a specialist in high-tech or computer-enabled crimes.

Finally, as a matter of prioritization, DPS makes attacks against government networks its highest priority. This is in part due to the sensitivity of information that government databases can contain. Governments are attacked very frequently by hacktivists because they are considered high profile targets.

Working With a State Legislature

Promising Practice: Work With Your Legislature to Build Support for the Program and its Priorities

DPS has been able to create a cyber program in a relatively short period of time (starting in 2012), in part because it worked with partners in the Utah legislature to make investigating cyber crime a priority. Many state-level cyber security experts report that they have never worked with their state legislators on cyber issues,[42] which can have a profound impact on funding for cyber security and cyber crime investigative efforts. The Utah state legislature knew that cyber crime is a significant problem, but DPS needed to make a concerted effort to educate the legislature about its need for funding.

With help from intelligence analysts at DPS's Statewide Information and Analysis Center (SIAC) and technical experts from the state Department of Technology Services (DTS), DPS produced an analysis of the current climate for cyber crime, as well as predictions for the future growth of cyber crime. SIAC personnel created a succinct presentation predicting a proliferation of cyber crime, which they delivered to the legislature.

DPS asked for dedicated funding to staff two-full time cyber crime investigators in addition to a cyber crime analyst, and in 2012, the legislature provided more than was requested by approving funding for three investigators and a civilian analyst.

[42] For example, nearly one third of state chief information security officers reported in a recent survey that they have no contact with their state legislatures. Robinson, Doug, and Srini Subramanian, Deloitte-NASCIO Cybersecurity Study: State Governments at Risk: Turning Strategy and Awareness into Progress, Deloitte University Press (September 2016), at p. 3. https://dupress.deloitte.com/content/dam/dup-us-en/articles/3470_2016-Deloitte-NASCIO-cybersecurity-study/2016-Deloitte-NASCIO-Cybersecurity-Study.pdf.

One of the Department's key champions at the state legislature was Representative Eric Hutchings (R - Kearns) who has been a victim of Internet-based identity theft. In an infamous incident, a criminal in Texas charged approximately $80,000 worth of telephone equipment to him, which Hutchings noted is the amount equivalent to about 16 typical bank robberies.[43] Ultimately, the losses suffered by the telephone equipment company were reimbursed by its insurance policy.

"What a wonderful criminal environment to be in, where people don't even look for you," Hutchings said. "If you rob 16 banks, you would be on the FBI's most wanted [list]. You rob it out of my credit [card], 'Eh, whatever, it's the cost of doing business.'"[44]

Importantly, the executive branch in Utah is supportive of DPS's cyber initiatives as well. "We are fortunate to have a supportive partner in Governor Gary Herbert who understands the crucial role that police play in investigating and preventing cyber crime," said Commissioner Squires.

For state and local police agencies looking to expand their cyber crime investigative capabilities, educating state officials about the importance of cyber issues can be a good first step to obtain funding. State legislators may be under the false impression that there is extensive federal grant money or federal investigative resources available to help local and state police. Unfortunately, that is not the case. It is an important leadership responsibility of state and local police executives to make their legislators aware of the needed resources to combat cyber crime.

Promising Practice: Rethinking Existing Criminal Codes to Reflect the Impact of Computer-Enabled Crimes

Police executives also need to work with their state legislators to strengthen criminal laws against cyber crimes and computer-enabled crimes. Technologies that enable cyber crime and the use of computers to commit traditional crimes are changing constantly, so it is challenging to update laws to reflect these changes. Many crimes like network intrusion are classified as misdemeanors.[45] For example, it can be difficult to prove that persons running a tech support scam are breaking the law, because they might be providing a minor service to their "customers" or they may refund money to customers who complain. Because of the time and investment that it takes to prepare a case against a perpetrator of a cyber crime, it can be frustrating for investigators if investigations result only in probation or minimal jail time.

Light criminal penalties may be partly responsible for the proliferation of some high-tech or computer-enabled crimes. If a crime has the potential for significant financial gain, a low likelihood of being investigated, and minimal punishment under the law if the perpetrator is caught, that is a ripe environment for these crimes to continue and expand. There is a need at both the state and federal levels

---

[43] Lee Davidson, "Massive Utah cyberattacks—up to 300 million per day—may be aimed at NSA facility," *Salt Lake Tribune* (February 25, 2016). http://www.sltrib.com/news/2135491-155/massive-utah-cyber-attacks-may-be.

[44] *Ibid*.

[45] For a comprehensive list of state criminal codes for network intrusion and related crimes, see National Conference of State Legislatures, "Computer Crime Statutes." http://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx.

for legislatures to update laws to reflect changes in technology and the severe harmful impact that high-tech crimes can have on victims.

For example, in the case of swatting (i.e., making a hoax call to local emergency services claiming that a serious crime, such as a murder or hostage-taking, is being committed at the home or business of the swatting victim), many cyber investigators—including those in the DPS Cyber Crimes Unit—felt the current sanctions are inappropriate. Swatting essentially is intended to cause police to send SWAT teams or other critical resources to what they believe is a major crime scene when in fact there is no crime being committed. This can be dangerous to the responding police officers as well as to the swatting victims who may panic when police suddenly arrive and try to gain entry in order to respond to what they believe is a critical incident. Computer programs that enable swatting to be done anonymously, which are easily accessible on the Internet, have contributed to increases in swatting incidents.

Swatting can be prosecuted as the crime of making a hoax police call, which currently exists under many state criminal codes. But in most states, making a hoax emergency call is a misdemeanor punishable with relatively small fines or potential jail time. These minor sanctions are inappropriate, considering that swatting can endanger victims and responding police officers.

As a result, legislatures across the country are beginning to draft bills to increase penalties associated with swatting.[46] Many of the measures contain the following provisions: making swatting a felony offense, imposing strict liability for any actions resulting in serious bodily injury or death, stiffening penalties for hoax calls that happen during times of emergency, and stronger penalties if a bomb or weapon of mass destruction is alleged to be involved. Recent legislation also provides mechanisms for requiring those convicted of swatting to reimburse victims and government agencies.

At the federal level, there have been several recent bills in Congress to increase criminal penalties associated with swatting.[47] Representative Katherine Clark (D-Massachusetts), who sponsored a swatting bill in the U.S. House of Representatives, was the victim of a swatting hoax in 2016, following her bill's introduction.[48] Across the country, several legislators who have advocated increasing criminal penalties for swatting have been targeted.[49]

The DPS Cyber Crimes Unit works to educate the Utah legislature on trends in cyber crime in order to ensure that the criminal code is amended to deter this type of criminal behavior.

The Utah legislature is currently considering a bill that would greatly stiffen penalties for swatting and several other cyber crimes, including denial-of-service offenses and "doxing."[50] The bill defines swatting

---

[46] "NJ Assembly passes bill cracking down on 'swatting,'" Associated Press (June 12, 2015). https://www.policeone.com/legal/articles/8569104-NJ-Assembly-passes-bill-cracking-down-on-swatting .

[47] See S. 1018 (The "SWAT Act" of 2015) and H.R. 4057 ("The Interstate Swatting Bill of 2015).

[48] Joshua Miller, "Police swarm Katherine Clark's home after apparent hoax," *The Boston Globe* (February 1, 2016). https://www.bostonglobe.com/metro/2016/02/01/cops-swarm-rep-katherine-clark-melrose-home-after-apparent-hoax/yqEpcpWmKtN6bOOAj8FZXJ/story.html.

[49] Patrick McGreevy, "Senator with anti-swatting bill is victim of hoax emergency call," *L.A. Times* (April 19, 2013). http://articles.latimes.com/2013/apr/19/local/la-me-pc-senator-swatting-20130419.

[50] H.B. 225 "Cybercrime Amendments." http://le.utah.gov/~2016/bills/static/HB0225.html.

calls involving alleged weapons of mass destruction as felony offenses and would allow judges to order restitution for costs associated with swatting. The bill also creates specific statutes criminalizing denial of service and doxing, increases penalties for network intrusion, and requires state agencies to report all intrusions to DPS for investigation.

[Page Intentionally Blank]

Understanding the Special Nature of Cyber Investigations

Changing the Culture of Your Agency

Lesson Learned: Expanding into Investigations Requires Police Departments to Educate Partners on How to Change their Thinking

Forensic evidence is essential for high-tech investigations. So police agencies looking to prosecute cyber attacks need to educate personnel in their own agencies and other organizations regarding digital evidence.

Information technology (IT) professionals at organizations that are victims of cyber crime might be tempted, for instance, to simply reimage a computer that has been infected with malicious software, wiping it clean and reinstalling the necessary programs so that it can be used safely. This comes at a high cost, however, because any evidence that might have been on the machine would be destroyed in the process.

Cyber criminals destroy digital evidence that may be used against them, which is something that cyber investigators should be trained to anticipate and guard against. For example, portable electronic devices (PEDs) such as tablets and cell phones can be "wiped" remotely if they are connected to a network or the Internet. Incriminating files and software are deleted. As a result, investigators must be trained to think proactively, so when they recover PEDs, they quickly place these devices in airplane mode, preventing them from connecting to any network. Simply turning PEDs off is not recommended, because as soon as they are turned back on, they reconnect to the network and can be accessed (and therefore wiped) remotely.

This need to consider defensive strategies and investigative thinking extends to police agencies' own IT departments. IT staff members are often involved in cyber crime investigations as subject matter experts for cyber crime investigators or as guardians of police agencies' networks to prevent and respond to cyber attacks. Even though cyber crime investigators are extensively trained and typically are assisted by civilian cyber crime analysts in their work, IT professionals are another invaluable resource for investigators. For high-tech crimes like network intrusion, for instance, an investigator must understand which defensive cyber security measures are in place in order to determine how a network was breached.

While an IT professional's first priority is defending the network of their employing organization, IT professionals working with cyber crime investigators need to also understand the importance of securing evidence for investigations.

With this in mind, Commissioner Squires advises any police department looking to start a cyber investigative function to help IT staff at public and private partner agencies consider the forensic (and legal) importance of digital evidence.

In Utah, a centralized IT department, the Department of Technology Services (DTS), protects all state agencies' various networks from breach. When DPS investigators are investigating cyber attacks against Utah state agencies, it is much easier to work with one IT department on standardized networks. This centralization also facilitates dissemination of best practices and training of IT personnel.

In place of DTS's IT staff's past practice to wipe an affected network clean to remove the threat, following the creation of the Cyber Crimes Unit and emphasis on actively investigating cyber incidents, staff are now trained to properly preserve forensic digital evidence.

Digital Evidence: Prioritizing Tasks to Help Digital Evidence Reach its Full Potential

In July 2014, RAND and PERF held a workshop, with support from the National Institute of Justice, in which police, prosecutors, academics, and privacy experts discussed issues related to digital evidence. Participants discussed the most pressing needs for innovation to help law enforcement agencies realize the full potential of digital evidence in the criminal justice system.[51]

There was a list of "top-tier" issues that participants agreed were the most pressing needs.[52] The top needs identified were:

- **Prosecutors need to be educated on making more focused uses of digital evidence.** The police experts agreed that many prosecutors lack knowledge of digital evidence, which leads them to request greater evidence extraction than may be necessary for a case, bogging down digital evidence examiners.
- **Judges need a better understanding of the issues surrounding the admissibility and use of digital evidence at trial.**
- **First-responding patrol officers and detectives need better training to understand where digital evidence may be present at the scene of an incident.** Training should cover the obtainment, chain of custody, and admissibility of digital evidence found at an incident or arrest. Digital evidence training for all first responders can also help limit the collection of evidence that is not relevant to an investigation.
- **Police agencies should provide better prioritization and triage analysis of digital evidence, given the scarcity of available resources.** Because most police agencies do not have enough personnel to process digital evidence, departments should look into tools and guidelines to reduce backlogs and help digital evidence examiners prioritize work flows.
- **Nationwide, police agencies should develop regional models to share digital evidence analysis capabilities.** Particularly for small agencies that have limited funds for specific tools or software, sharing tools with other agencies in the region can be an effective way to enhance capabilities.
- **Police agencies need to address concerns about maintaining the currency of training and technology**. As technology changes rapidly, there is a constant need to reassess the appropriate investment in investigators' training and tools. As one official said, "You can't be a high-tech task force running yesterday's technology."

[51] Sean E. Goodison, Robert C. Davis, and Brian A. Jackson, Digital Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence, RAND Corporation (2015). https://www.ncjrs.gov/pdffiles1/nij/grants/248770.pdf.

[52] Participants agreed on which needs were top-tier using the *Delphi* method developed by RAND Corporation. *Ibid*.

While there has been vast improvement in many police agencies to incorporate technology and explore digital evidence capabilities, there is still more work to be done to fully capitalize on the investigative and prosecutorial potential of digital evidence.

Legal Considerations

For most jurisdictions, many unresolved questions exist about how to handle digital evidence. Technological advances frequently outpace the course of legal doctrine, and it can be challenging for investigators, prosecutors, defense counsel, and judges to resolve issues involving digital evidence when there are issues that are too new to have produced any legal precedents. Recent jurisprudence recognizes that technology has significantly altered the way that people store private information about themselves.[53] However, there often remain unresolved questions on how to apply technological changes to existing legal standards, including:

- How should law enforcement agencies ensure proper authentication and chain of custody for the admission of digital evidence in court?
- How can police draft search warrants with sufficient particularity when the location of inculpatory or exculpatory evidence on a computer network or personal electronic device may not be obvious until the network or device is searched?
- How can investigators limit their search of computers or devices when many digital forensic tools require examiners to "dump" the entire contents of a computer, phone, or other device?
- How should law enforcement agencies best handle the discovery of obvious contraband under the "plain view"[54] doctrine while in the course of a digital examination (e.g., should they be required to obtain a separate search warrant)?
- With rapid changes in technology, how can police prove that digital examination techniques have the scientific acceptance required for admission in court? How can law enforcement agencies cull voluminous digital evidence in a fast and easily digestible fashion to satisfy obligations to turn over exculpatory evidence to the defense?
- Under the Fifth Amendment's prohibition against self-incrimination, how and when can law enforcement agencies compel criminal suspects to provide passwords to police or unlock their devices? Can law enforcement agencies send those requests to technology companies or to an employer who may own the phone?

[53] In *Riley v. California,* the Supreme Court held that warrantless searches incident to arrest of portable electronic devices were unconstitutional. 134 S. Ct. 2473 (2014). In doing so, the Court recognized the potential for cell phones to carry vast quantities of sensitive or private information such as photographs, email messages, contact information for friends and business associates, bank statements, prescriptions, and browsing histories of Internet sites. The Court held that "the fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought."

[54] The plain view doctrine allows a police officer in some circumstances to seize evidence or contraband that is in plain sight without obtaining a search warrant. See *Coolidge v. New Hampshire*, 403 U.S. 443, 465 (1971).

Legal disputes over these types of issues are playing out in the courts and the news media. For example, during the FBI's investigation of the 2015 San Bernardino shooting, agents recovered a locked smartphone used by one of the suspects. After exhausting its resources, the FBI asked the phone's manufacturer, Apple Inc., for help in accessing the phone's contents. Apple publically refused the request, saying it had already aided the FBI's investigation to the greatest extent of its legal responsibility.

Apple executives testified before Congress that the FBI's request for backdoor access to the mobile device amounted to an unconstitutional breach of a user's privacy rights, and argued that honoring the request would set a dangerous precedent. In response, the FBI secured a court order in an attempt to legally compel Apple to help, which Apple challenged. After a months-long public debate, the Department of Justice (DOJ) eventually abandoned its order for Apple to comply, announcing that it had succeeded in accessing information on the device through alternative means.

Throughout the debate, Apple executives maintained their commitment to aiding law enforcement investigations, noting in an open letter to their customers that Apple engineers had already provided assistance to federal investigators in the San Bernardino case.[55] However, the company claimed that the FBI crossed a legal boundary by asking Apple to create a "master key" for its devices. While the FBI said it was interested in a one-time-use fix, Apple executives believed that creating such a "workaround" would be extremely dangerous in the hands of a cyber criminal. FBI Director James Comey refuted characterizations of the request as a backdoor to access customer data in circumvention of user-controlled security protocols, but Apple CEO Tim Cook argued that not even Apple itself should have direct access to a user's private data.[56]

[55] Tim Cook, "A Message to Our Customers" (February 16, 2016). http://www.apple.com/customer-letter/.
[56] Seth Rosenblatt, "FBI director demands access to private cell phone data," Cnet (October 16, 2014). http://www.cnet.com/news/fbi-director-demands-access-to-private-cell-phone-data/.

Microsoft has also engaged in a lesser-known dispute with federal investigators. In 2013, the Department of Justice secured a search warrant for emails and account information held on Microsoft's "MSN" server. While details of the case have been sealed, CNN Money reported that investigators were seeking account information as part of a drug dealing investigation.[57] Microsoft, citing the server's overseas location in Ireland, challenged its legal responsibility to hand over the information.[58] The company's lawyers argued that DOJ does not have the authority to subpoena records stored outside of the United States, and thus it would have to go through a lengthy process with Irish officials under a Mutual Legal Assistance Treaty (see "*The Formal Process: Mutual Legal Assistance Treaty (MLAT) and Extradition Requests"* section for more information). In July 2016, the Second Circuit sided with Microsoft, quashing the warrant.[59]

Lesson Learned: Cyber Investigations May Require More Time Than Other Major Crimes

In many respects, conducting a cyber investigation requires the same skills as other major criminal investigations, but cyber crime investigations also present unique challenges. Commissioner Squires noted that cyber investigations require significantly more time, for two reasons. First, it often takes a substantial amount of time to vet a cyber investigative lead, to see if one can open a criminal case. Second, the building blocks of collecting digital evidence, including sending subpoenas to private companies such as Internet service providers (ISPs), can take months to produce replies. Soliciting information from foreign entities, through mutual legal assistance treaties, complicates matters further.

Investigators also must overcome challenges associated with the anonymity of the Internet to use traditional investigative techniques that can close cases and build cyber intelligence. For example, police agencies are looking to develop networks of confidential informants connected to the dark web and finding ways to reward people who come forward to report cyber crimes.

DPS begins its cyber crime cases by interviewing the complainant to verify information. Investigators attempt to determine the dollar loss and whether there is any evidence that could result in the identification of a suspect.

---

[57] David Goldman, "Microsoft is fighting the DOJ too," CNN Money (February 23, 2016). http://money.cnn.com/2016/02/23/technology/microsoft-ireland-case/.

[58] Brief for Appellant, *Microsoft Corporation v. United States of America*. 14-2985-CV. U.S. Court of Appeals for the Second Circuit. Filed December 8, 2014. http://digitalconstitution.com/wp-content/uploads/2014/12/Microsoft-Opening-Brief-120820141.pdf.

[59] *Microsoft v. United States*, No. 14-2985 (2nd Cir. 2016). http://pdfserver.amlaw.com/nlj/microsoft_ca2_20160714.pdf.

After interviewing the complainant, investigators assess whether the case can be solved. They assess the amount and quality of any evidence, whether there are suspects, and the severity of the crime. The investigator then reaches a conclusion, which is reviewed by the Cyber Crimes Unit Sergeant.

The vetting process before opening a case is perhaps one of the most distinguishing aspects of cyber investigations. The DPS Cyber Crimes Unit relies heavily on its civilian cyber intelligence analyst housed at the SIAC to make these determinations. The cyber intelligence analyst collects information related to potential cyber incidents and analyzes that information to determine whether there is a criminal nexus or intelligence value (for example, the particular tradecraft or *modus operandi* of a specific hacking group that may enable its identification or prosecution at a later date). If the cyber intelligence analyst determines there is a criminal nexus, he or she advises investigators about whether there is enough evidence to open a criminal case. The cyber analyst's process in handling information is shown in figure 2.

The boxes at the top left of the diagram represent referrals or tips of cyber incidents that may need to be analyzed for criminal investigative purposes or as intelligence. Referrals come in the form of digital evidence of a cyber crime (often visible in the firewall or application log files), incident reports from a variety of partners, network packet captures (showing data moving across and therefore attacking a computer network), or tips/leads from IC3. After a referral is received, the cyber intelligence analyst conducts a preliminary analysis of the information to determine whether there is a criminal nexus or intelligence value to the data.

If there is probable cause to believe that a crime has occurred, information will be entered in the DPS's case tracker system for vetting by the cyber intelligence analyst and investigators to determine whether investigators will open a criminal case. Even if the evidence does not have a criminal nexus, there may still be an intelligence value; for example, a description of a tradecraft or technique that a particular cyber attacker employs that has not yet been seen in Utah. If there is intelligence value to the data, the cyber intelligence analyst will determine whether it constitutes actionable intelligence and the best format (e.g., intelligence product) for dissemination among information sharing networks like the Utah State Cyber Intelligence Network. Intelligence is stored and retained in a catalog, which is subject to the data retention requirements of 28 C.F.R. Part 23 and must be reviewed to determine whether the SIAC will purge or retain it.

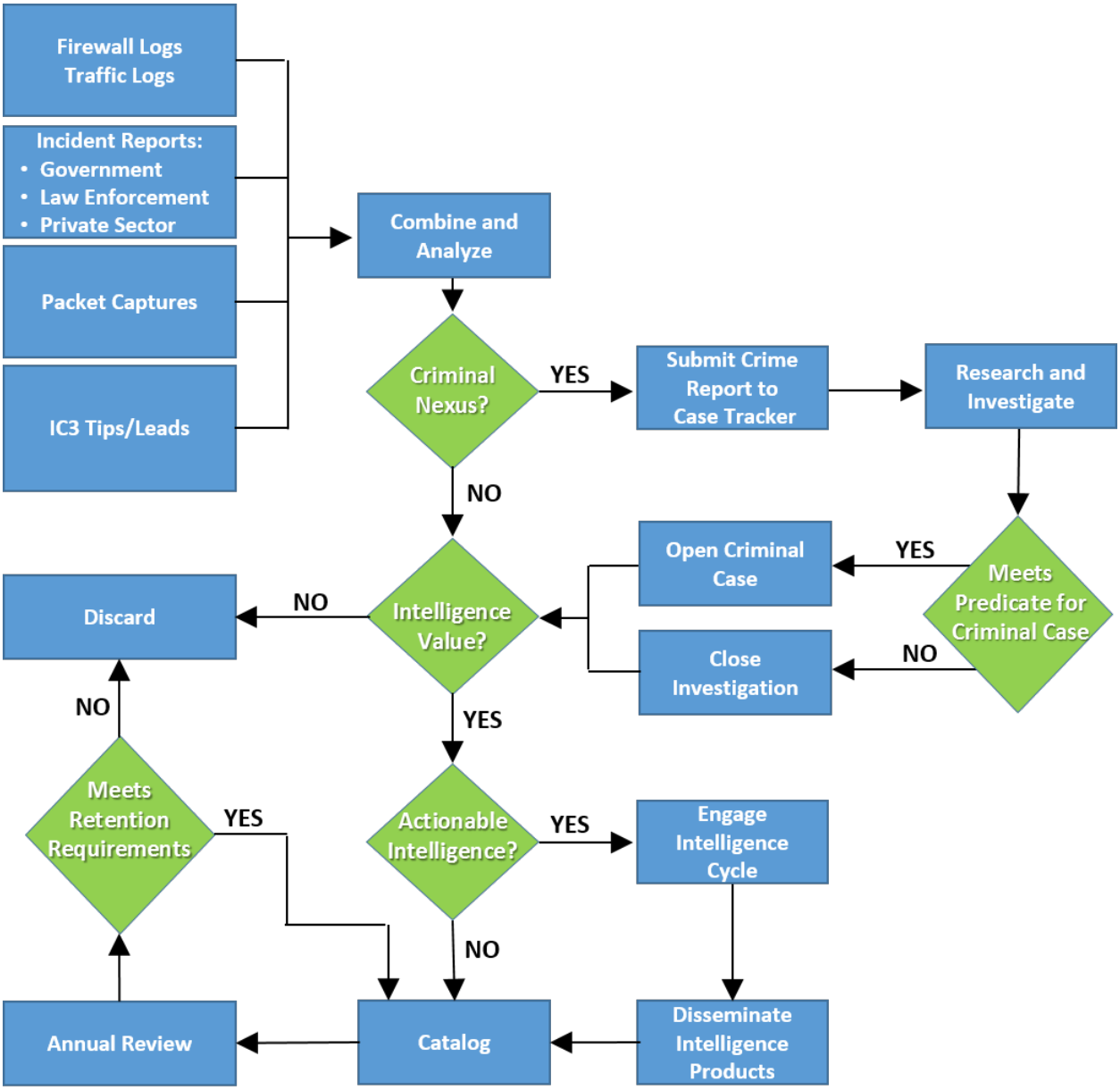


Figure 2: The Cyber Intelligence Analyst's Work Flow[60]

[60] Utah Department of Public Safety, "Establishing a Cyber Crimes Unit," White Paper (September 11, 2014), at 8. http://docplayer.net/10626312-Establishing-a-state-cyber-crimes-unit-white-paper.html.

The cyber intelligence analyst prioritizes assignments in a very specific order. To alleviate concerns about the length of time taken in investigations, the first priority is vetting investigative leads and investigators' requests for assistance on active cases or active intelligence. The second priority is producing intelligence bulletins and reporting to federal agencies. Finally, the cyber intelligence analyst's third priority is to conduct outreach—both to law enforcement agencies in Utah and through the public outreach information liaison officer program to public and private cyber-partners.

The Association of State Criminal Investigative Agencies' Work to Improve Cyber Investigations and Intelligence Operations

With a mission to facilitate information sharing and collaboration, and thereby address the complexities inherent in cyber crime, the Association of State Criminal Investigative Agencies (ASCIA) formed a Cyber Working Group in 2016. Chaired by New Jersey State Police Lieutenant Colonel Raymond Guidetti, the committee consists of representatives from 43 states who supervise cyber operations for their respective agencies. The committee draws on the collective experience and functional knowledge of its members to bring insight to cyber matters that range across a spectrum of investigative and intelligence efforts.

The committee hosts monthly web conferences to discuss cyber trends, actively disseminates information, and promotes effective practices among its members. In cooperation with the Bureau of Justice Assistance and the National White Collar Crime Center, ASCIA also supported a 2-day Cybercrime Consortium meeting in Dallas, Texas. This important forum enabled state partners to discuss issues that impede their ability to investigate and prosecute cybercrime, and several recommendations and action items were the result of this meeting.[61] The committee has also implemented a mechanism for deconflicting cyber investigations and intelligence operations on a national level. At the time this report was published, the system was undergoing field testing.

Records collected from software companies, cell phone carriers, and Internet service providers are often essential for establishing a criminal case against perpetrators of high-tech and computer-enabled crimes. However, these companies respond to law enforcement on different time schedules. While some prioritize law enforcement requests, particularly under exigent circumstances, wait times can be quite substantial. Investigators regularly noted that record requests may take several weeks when they have a warrant, and often several months if investigators are requesting information with a subpoena. Practically speaking, by the time that information comes back from private companies, it may be unusable.

[61]Bureau of Justice Assistance, 2016 State of the States Cybercrime Consortium Report.

Police executives looking to create their own cyber crime units should understand the unique aspects of high-tech and computer-enabled crimes. For example, due to the delays in collecting digital evidence and vetting leads and tips, building a case against a cyber criminal may take longer than cases against other kinds of offenders. As a result, cyber units may produce fewer arrests per year, relative to other units.

Personnel, Management, and Performance

Police Agencies Need Creative Means to Define Success in Cyber Investigations

Police agencies must implement alternative measures to assess the effectiveness of their cyber crime units. Clearance rates, for example, may be an effective means to track the progress of investigative units for more traditional crimes, but in the realm of cyber crime, difficulties in obtaining evidence or reaching perpetrators overseas make traditional metrics insufficient for capturing the overall success of a cyber program. Major Brian Redd, Director of the State Bureau of Investigation, said that "while measuring success can be difficult for all law enforcement agencies, it is particularly difficult when it comes to cyber investigations." In 2015, the DPS Cyber Crimes Unit opened 116 criminal cases related to high-tech or computer-enabled crime, but this came from a far larger number of referrals.

In addition to successful prosecutions, cyber unit success can be defined in other ways. For example, if an investigation leads to a disruption of a major criminal network, police agencies should capture this outcome. Even if a perpetrator is not identified, investigations that enable victims to recoup losses or prevent additional financial losses should also be tracked. Investigations also go hand in hand with cyber intelligence and cyber security. If an investigation results in the dissemination of a key piece of intelligence for law enforcement, government, or private-sector partners, or allows IT professionals to strengthen network defenses, that should also be considered a successful investigation, even if no arrest is made. In that sense, it is important to view cyber crime investigations as similar to shifts in other policing efforts that focus on crime victims. Law enforcement agencies like Utah's DPS are working to implement a victim-centered, preventative approach, rather than focusing solely on arrests.

> **"You can't define success in cyber by the number of handcuffs you put on people."**
>
> ***—Commissioner Keith Squires, Utah Department of Public Safety***

As a practical matter, however, funders like state legislatures or governors' offices are looking for documented progress in order to justify renewing funding. Therefore, DPS investigators are capturing metrics that help assess the effectiveness of the unit, keeping in mind the victim-centered, preventative approach that reflects the complexities of cyber crime investigations. DPS is now tracking:

- Training—including requests for assistance from or technical assistance provided to local law enforcement partners
- Recoveries—dollar amounts recovered from perpetrators of cyber crime
- Prevention—financial losses that DPS was able to prevent from happening
- Intelligence—the number of raw intelligence reports, products, and situational awareness bulletins produced
- Cases—numbers of types of cases investigated and overall total active cases
- Hours spent—vetting investigative leads or working on active cases
- New cyber security defenses achieved—particularly those that can protect state networks and be disseminated to private-sector partners in the Utah State Cyber Intelligence Network

For example, since its inception, the DPS Cyber Crimes Unit has recovered approximately $3 million. This includes fraudulent wire transfers that the unit was able to freeze and stop, and the return of expensive equipment in a shipping fraud case.

Staffing and Personnel Issues

Police agencies must determine which investigators will work cyber cases. DPS investigators noted that it often takes about 6 months for new investigators to be fully trained, and it can take a year or longer for them to acquire enough experience to feel comfortable with the technical issues.

As a result, DPS requires its investigators to make a minimum 5-year commitment to the Cyber Crimes Unit. DPS chose investigators with varied backgrounds and levels of experience. Notably, only one of the detectives has a degree in computer science. Because DPS defines cyber crime to include computer-enabled fraud, several of the investigators have experience working fraud cases. Commissioner Squires noted that this background can be useful because fraud investigators, like cyber crime investigators, write large numbers of subpoenas. Other cyber crime units have also recruited investigators with backgrounds investigating financial crimes, which are similar to cyber crimes in terms of the amount of paperwork and diligence required.

Nationwide, police agencies that have created cyber crime units have worked to balance officers' promotional concerns against the length of time required to become proficient. Police executives differ on whether the ideal investigator should be young and likely more comfortable with new forms of technology or whether ideal investigators should be closer to retirement (and potentially less concerned with promotion), so that they may be more willing to spend 5 years or more in a cyber unit.

Police agencies with established cyber crime units also note that losing investigators and civilian analysts to the private sector is a common phenomenon. One benefit to this turnover, however, is that it can be advantageous to have former police officers working for private-sector partners that assist with information-sharing efforts. For example, groups like the Microsoft Digital Crimes Unit, whose staff

include former police officers, can provide case referrals and crucial information on cyber threats to local and state police agencies.[62]

For performance reviews, command staff at SBI noted that they have started to use case hours as a marker for personnel considerations. Cyber investigators will have their performance evaluated based on the number of hours spent conducting case assessments, hours spent working on active cases (which they will compare to other SBI investigators), and hours spent working with other government agencies like the Department of Technology Services or with private-sector organizations.

Lesson Learned: Personnel Who Work on Cyber Investigations Are Vulnerable to Personal Attacks

Commissioner Squires quickly learned the lesson that personnel in his agency—particularly those who work on high-tech crime investigations—are vulnerable to cyber attacks. Cyber attacks from politically motivated hacktivists have been an issue for DPS. This has also been the experience of other police agencies.

In 2015, a local police department in central Utah experienced a police-involved shooting that garnered media attention. A trooper with the Utah Highway Patrol responded to the scene in a marked police vehicle that the media captured in photos and later released to the public. Even though the officer who was involved in the shooting was not a member of the Utah Highway Patrol, hacktivists saw the photo and decided to "dox" the colonel at the helm of the Utah Highway Patrol, putting personally identifying and sensitive information on the Internet, which led to his personal bank account and credit card numbers becoming compromised.[63]

Commissioner Squires feels that each law enforcement agency must help to ensure the online and personal safety of its officers by, for example, allocating specific funding for identity protection services for personnel. Indeed, Commissioner Squires purchased identity theft monitoring for the individual involved in the doxing incident. In the future, officer wellness programs should aim to address the digital exposure that officers can face from cyber criminal or politically motivated hacktivists.

Personnel who work cyber crime investigations must be prepared for the potential that they could be doxed. Agencies can help officers by training investigators about the potential consequences, offering remediation services such as repairing credit scores, and helping educate them about prevention techniques that can reduce the amount of personal information available online. While many officers are willing to accept the potential consequences of cyber attacks, fear of retribution can have an especially negative impact on civilians such as IT professionals who testify in court. While no police agency can fully protect its officers from cyber attacks, it is important for police executives to understand the challenges that their personnel may face.

---

[62] Ciara O'Brien, "Microsoft leading the fight to counter cybercrime," *The Irish Times* (March 10, 2016). http://www.irishtimes.com/business/technology/microsoft-leading-the-fight-to-counter-cybercrime-1.2566206.
[63] Lee Davidson, "Massive Utah cyberattacks—up to 300 million per day—may be aimed at NSA facility," *The Salt Lake Tribune* (February 25, 2016). http://www.sltrib.com/news/2135491-155/massive-utah-cyber-attacks-may-be.

Leveraging Partnerships

The Value of Partnering with the FBI

Lesson Learned: No Agency Has the Resources to Address Cyber Crime Alone

State and local agencies may be tempted to assume that cyber crime falls under federal jurisdiction and is therefore not a state or local priority. However, state and local cyber programs show that no single agency can address all cyber crimes. It can be particularly challenging for the FBI, which is often tasked with prioritizing cyber terrorism and crime conducted by nation states, to delve into computer-enabled crimes that do not involve a large financial loss. In fact, the FBI field offices must necessarily impose a threshold for monetary losses when deciding whether to open an investigation.

> **"If we can free up the FBI's investigators and resources to work on national security and terrorism cases, then that alone makes our participation worth it."**
>
> ***—Commissioner Keith Squires, Utah Department of Public Safety***

Operation Wellspring began in 2013 as a pilot program for DPS and the FBI's Salt Lake City Field Office to leverage each other's resources, capabilities, and focus areas. For the FBI Salt Lake City Field Office, the benefits of partnering with DPS were enormous. The supervisory special agent for cyber had additional officers who were able to investigate some of the cases which the FBI could not include in its case load. Operation Wellspring also ensured that an entire category of crimes that might otherwise go unaddressed, specifically computer-enabled financial crime with smaller monetary losses, were investigated.

For DPS investigators, partnering with the FBI had several important benefits that enabled the cyber unit to be effective: 1) the FBI provided the essential multi-jurisdictional reach needed to address cases where the victims or perpetrators were located outside of Utah; 2) the FBI provided hands-on training and mentorship for complicated technical skills; and 3) the FBI's database gave access to crucial information for vetting and investigating cases, as well as exploring potential associations among separate cyber incidents.

The relationship also allowed for crucial deconfliction of efforts. In some cases, a victim of a cyber crime might report to one or more of the following: their local police agency, the FBI, or IC3. Particularly because cyber crime investigations are so lengthy and extensive, it is crucial for agencies to share information to reduce redundant efforts.

In order to provide DPS cyber investigators and analysts access to the FBI database, the federal government required that all personnel submit to a background check and obtain a TS-SCI security clearance. For other jurisdictions considering implementing the Operation Wellspring model, there is a

need to look well ahead for succession planning to account for changes in personnel during what can be a lengthy clearance process.

Importantly, one of the aspects that distinguishes Operation Wellspring from a more traditional joint task force is that the partnership comes with no dedicated funding attached. Even though this means that DPS must pay salaries for three dedicated cyber investigators who are stationed offsite at the FBI's office, Commissioner Squires understood the value of working together. So other jurisdictions looking to partner with the FBI on cyber investigations should be prepared to secure funding for their investigators.

In the first year of the Operation Wellspring pilot, IC3 provided the DPS Cyber Crimes Unit with approximately 25 case packets for review, which involved over 900 victims and $2.5 million total in losses.[64] From those referrals, DPS opened 9 cases for investigation and the FBI initiated 14.[65] FBI Director Comey declared the pilot for Operation Wellspring a success based on the following promising results reported by DPS and FBI personnel:

- Pooling resources to better address cybercrimes at both the federal and state levels
- Increasing the investigative abilities and productivity of all partner agencies
- Building partnerships that increase coordination thereby deconflicting duplicative efforts and enhancing capabilities[66]

As of November 2016, the initiative has expanded to the following nine locations: San Diego, Oklahoma City, New York, Buffalo, Phoenix, New Orleans, Albany, Knoxville, and Kansas City, Missouri.

Promising Practice: Working with the FBI Provides Many Benefits for State and Local Cyber Investigators

Partnering with the FBI enabled the Cyber Crimes Unit to effectively address many more cases because of the FBI's wide jurisdictional reach. It is rare that in either high-tech or computer-enabled crime, the perpetrator and the victim live in the same jurisdiction. Limiting the jurisdiction to the state of Utah in the first year of the Cyber Crimes Unit's existence severely hampered the team's ability to investigate many leads.

For Commissioner Squires, partnering with the FBI was a promising practice that provided an answer to the multi-jurisdictional nature of cyber crime. Because of DPS's role as a state law enforcement agency, the Commissioner said that DPS has strong relationships with local law enforcement agencies in Utah and other departments throughout the region. These relationships developed as investigators from different agencies worked cases together. In some cases, cyber investigations led to suspects or middlemen in a different region of the country. Commissioner Squires said the FBI assisted by introducing his investigators

[64] Utah Department of Public Safety, "Establishing a Cyber Crimes Unit," White Paper (September 11, 2014). http://docplayer.net/10626312-Establishing-a-state-cyber-crimes-unit-white-paper.html.
[65] *Ibid.*
[66] Keith D. Squires, "Cybercrimes Enforcement: A State Perspective," *The Police Chief* 81 (February 2014), pp. 42–45. http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display&article_id=3268&issue_id=2201.4.

to cyber investigators throughout the United States, who otherwise might have been difficult for investigators in Utah to identify and contact.

Partnering with the FBI also provides other benefits for state investigators. State investigators are paired with FBI agents who can serve as mentors on cases with difficult technical issues. This hands-on aspect allows investigators to develop skills more quickly. Because state investigators complete a security clearance process, they are able to access FBI databases that contain a wealth of intelligence on cyber incidents. Finally, the partnership with the FBI allows state investigators to receive IC3 case packets, which help in their investigations of cyber incidents. IC3's referrals can help identify connections that would otherwise be missed in order to "connect the dots" and aggregate cyber offenses, giving a more complete picture of the totality of a criminal actor's or organization's impact.

The Nigerian Purchase Order Fraud Case: A Spotlight on State and Local Agencies' Involvement in International Cases

One of the biggest challenges that the Department of Public Safety identified in its cyber work is the international component of cyber crime. Cyberspace has no borders and allows offenders to connect from all parts of the world. The FBI currently estimates that approximately 95 percent of cyber criminals are foreign nationals who do not live in the United States.[67]As a result, it is extremely rare in many types of high-tech cases, and even in relatively simple computer-enabled crime cases, that an American victim of a cybercrime will live in the same jurisdiction as the perpetrator. However, DPS has been able to find ways as a state agency to leverage its partnership with the federal government to give its investigators an international reach.

In 2014, the DPS Cyber Crimes Unit was assigned to investigate a purchase order fraud that occurred against a computer company based in Utah. The FBI came to DPS investigators, providing them with the referral. The company reported that it received a purchase order from what appeared to be a legitimate business with which it had successfully completed orders in the past. The company delivered a large volume of computer hard drives and other expensive technological equipment on credit. After investigation, it became clear that a criminal actor had used information obtained illegally through the Internet to impersonate the legitimate customer.

The Cyber Crimes Unit followed the product in order to determine who perpetrated the fraud. Like many cyber cases, the criminal organization used a straw man (a person used as a cover for the criminal in a transaction) in an attempt to mask the destination for the merchandise. Investigators at DPS noted that this tactic is a common phenomenon in computer-enabled fraud cases, and these individuals often are not fully aware that they are involved in a criminal conspiracy. Criminal organizations engaging in cyber fraud have used sophisticated methods to recruit middlemen positions under the guise of legitimate businesses, sometimes even posting job vacancies and conducting in-person interviews.

[67] James Trainor, "Confronting Cyber Threats: Cybersecurity from the FBI's Perspective," The Massachusetts Attorney General's National Cyber Crime Conference, Norwood, MA. Keynote Address (April 25, 2016).

In this case, the criminal organization devised a complicated transaction. It had the product delivered to a middleman who was also being scammed in a jurisdiction in the United States that was under the watch of a different FBI field office. Actors in the scam received goods at a storage unit, and then sent the goods to a forwarding company run from a warehouse. Once there was enough product to justify the international shipping costs, the forwarding company sent a pallet of goods to Nigeria. After discovering the depth of the scam, the FBI was able to use its official channels—the legal attaché in Nigeria—to reach out to Nigerian police.

After working in close coordination with the FBI's Salt Lake City Field Office, another FBI field office, and eventually Nigerian police, DPS made an arrest. The Nigerian police sent a commander to Utah at the time of the investigation to collaborate with DPS on the case. Eventually, the FBI and Nigerian police conducted surveillance of the pallet coming into the country and were able to arrest three members of the organization, as well as a facilitator in South Africa. Importantly, the victim company located in Utah was able to recover its equipment, including hard drives and ultrasound equipment, from Nigeria.[68]

These types of cases demonstrate the unique value in creating state and federal partnerships to address a growing area of crime. Without the FBI, DPS would have had a difficult time identifying the suspects and coordinating all of the logistical and cooperative elements with international police partners. And without DPS manpower, commitment, and investigation, the FBI would not have had the resources to be able to pursue a case with relatively minor (in the realm of cyber) losses to the Utah victim company.

International Case With Cyber Allies

When an investigation leads to a suspect who is located in a foreign country, some allied countries, including Canada and the UK, are willing to share information. Several police agencies in the United States with robust cyber programs have, in fact, cultivated relationships with international counterparts to address cyber crime. The cooperation is essential to effective cyber investigations, because it helps overcome certain jurisdictional limitations.

Similar to the computer-enabled fraud case that DPS successfully followed to Nigeria, many other law enforcement agencies throughout the country have leveraged connections through their local FBI field office and FBI legal attachés to refer cases to police agencies in cyber-ally countries. For example, in a particularly troubling case, a detective sergeant from the Johns Creek, Georgia, Police Department investigated a swatting incident related to sexual harassment of a female gamer.[69] The perpetrator met the victim in an online gaming website called "Twitch" and followed through with a threat to dox and swat her if she did not speak with him when he wanted. The perpetrator called the police in Alpharetta, Georgia, stating that he had killed three people in a home and was holding a girl hostage, threatening to

[68] Nicole Blake Johnson, "Utah Cyberunit Tackles Crimes Below the FBI's Radar," *State Tech Magazine* (February 11, 2015). http://www.statetechmagazine.com/article/2015/02/utah-cyberunit-tackles-crimes-below-fbi-s-radar.
[69] Jason Fagone, "The Serial Swatter," *The New York Times* (November 24, 2015). http://www.nytimes.com/2015/11/29/magazine/the-serial-swatter.html?_r=0 .

kill the girl if he did not get $30,000. The police arrived at the woman's house in riot gear, frightening her and her family.

The police chief vowed to resolve the case after seeing the trauma that the SWAT raid had inflicted on the woman's family. Without any prior experience in cyber crime, the detective sergeant assigned to investigate the case made painstaking efforts to subpoena the VoIP providers associated with the call, and linked the case to a Skype account that made over 40 hoax emergency calls to police stations throughout the United States. He determined that the Skype account was associated with a juvenile living in Canada. Going through the Atlanta FBI Field Office and then the legal attaché in Canada, the detective sergeant prepared evidence and referred the case to Canadian police. The perpetrator had become so confident in his ability to evade law enforcement that he demonstrated several swatting incidents to a live audience on the Internet. Canadian police arrested the suspect, charging him with 46 counts of criminal harassment, public mischief, and extortion. The juvenile pled guilty to 26 counts and served 16 months in youth jail.[70]

These cases demonstrate the need to cultivate partnerships with international allies. In the realm of cyber crime, agencies must get accustomed to the idea that they will often spend a significant amount of time and resources on a case, and then hand it over to another jurisdiction to charge and prosecute. This may require a change in thinking from traditional police investigations in which the lead investigative agency handles the case.

> **"It does not matter to us who prosecutes our cyber crimes, so long as justice is served for our victims."**
>
> **—Major Brian Redd, Director of the Utah State Bureau of Investigation**

There are also technological challenges that make it difficult for allies to share information on high-tech crimes. Through programs like Operation Wellspring and joint task forces, state and local police agencies obtain access to important FBI databases that aggregate, sort, and analyze data. But there is no way that U.S. agencies can grant that same access to international partners, due to security concerns. Instead, the FBI must input massive amounts of raw data into special shared platforms for international partners, and those platforms are rather basic, with no organizational or search capability, which makes it challenging for users to analyze data and prepare evidence. There is therefore a need to improve cyber information-sharing platforms among partners to enhance analysis capabilities while maintaining security protections.

[70] *Ibid.*

The Formal Process: Mutual Legal Assistance Treaty and Extradition Requests

When an investigation leads to a perpetrator in a country that is not an ally of the United States, the process is even more complicated. All international FBI investigations must be coordinated through the FBI's legal attaché office in the subject country. But when the country is not an ally, the likelihood that the subject country will assist with investigations is reduced.

A Mutual Legal Assistance Treaty (MLAT) request is the official mechanism the United States uses to obtain evidence related to criminal activity from foreign countries. The requests are related to individual treaties that the United States has with most countries, which typically allow U.S. law enforcement agencies to move investigations forward through the following actions: obtaining testimony from witnesses; executing search warrants; obtaining bank records; and/or freezing assets.[71] If there is enough evidence to make an arrest, then the United States can formally request an extradition.

Even if there is no official treaty in place for mutual legal assistance, there are still protocols by which U.S. police officials can request information. As expected, in recent years, the number of MLAT requests coming both to and from the United States government has dramatically increased, particularly with requests related to computer records.[72]

Even if the country receiving the MLAT request has good diplomatic relations with the United States, the process is very time consuming. The President's Review Group on Intelligence and Communications Technologies[73]—whose mission is to provide recommendations on how to improve technical collection capabilities that impact national security and U.S. foreign policy— estimated that the average time to go through the MLAT process is 10 months, and some requests may take years.[74] This has led many activists and commentators to urgently call for reform of the MLAT process.[75] There are also complicated issues in the MLAT process related to privacy and whether recipient countries will give subjects sufficient due process.

In addition, countries can deny requests for various reasons—for example, in cases where an offense being investigated by the nation making the request under MLAT is not considered a serious crime in the nation receiving the request. Nations also vary in their general levels of cooperation. The ability to obtain

---

[71] See https://mlat.info/faq

[72] U.S. Department of Justice FY 2015 Budget Request, "Mutual Legal Assistance Treaty Process Reform." https://www.justice.gov/sites/default/files/jmd/legacy/2014/07/13/mut-legal-assist.pdf.

[73] President Obama established the Review Group in 2013 under the Director of National Intelligence to review and provide recommendations on communications technologies to optimally protect national security and U.S. foreign policy in a manner that protects privacy and civil liberties, recognizes the need to maintain public trust, and reduces the risk of unauthorized disclosure. See https://www.dni.gov/index.php/intelligence-community/review-group.

[74] Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies (December 12, 2013).

[75] Jonah Force Hill, "Problematic Alternatives: MLAT Reform for the Digital Age," Harvard Law School National Security Journal (January 28, 2015). http://harvardnsj.org/2015/01/problematic-alternatives-mlat-reform-for-the-digital-age/.

information and extradite cyber criminals is much lower for a country like Russia than for countries that have strong relationships with the United States.

Despite the obstacles in their path, U.S. law enforcement agencies are using a variety of strategies to apprehend cyber criminals, including conducting surveillance of suspects' international travel. For example, the U.S. government tipped off officials in Thailand to the presence of an alleged Algerian hacker who reportedly used malware called "SpyEye" to defraud banks of $100 million.[76] Thai officials arrested the suspect and extradited him to the United States where he pled guilty and was sentenced to 15 years in prison.[77] The Secret Service can also deploy undercover agents to encourage criminals to move across borders. A Secret Service undercover agent was credited with luring Maksym Yustremskiy ("Maksik") who was part of the criminal ring responsible for an $11-million breach of several U.S. retailers, including TJ Maxx, to a face-to-face meeting in Turkey where he was arrested.[78] Maksik received a 30-year prison sentence in Turkey.

Importantly for victims of cybercrime in the United States, there are also ways that the federal government can help prevent the loss of assets, even in cyber cases that originate in countries hostile to the United States. The federal government can assist agencies with freezing assets, in a process known informally as the "Financial Kill Chain," through a joint effort between the FBI and the Department of Treasury's Financial Crimes Enforcement Network (FINCEN). There are several requirements that need to be met in order to activate the Financial Kill Chain: 1) The losses must be greater than $50,000; 2) The case must involve an electronic transfer of stolen money to another country; 3) The loss must have occurred within the previous 72 hours; and 4) The victim must file a police report with a foreign law enforcement agency. If all conditions are met, the federal agencies can freeze funds in a foreign account. Typically, FINCEN's rapid response team or the FBI's legal attaché offices will reach out to law enforcement in the country receiving the funds or the relevant banks and ask them to freeze the funds for 3 days, thus allowing the sending bank to recall the wire transfer.

[76] Mark Clayton, "'Happy Hacker' arrest: Did police just nab a cyber crime 'botmaster'?" *The Christian Science Monitor* (January 10, 2013). http://www.csmonitor.com/USA/2013/0110/Happy-hacker-arrest-Did-police-just-nab-a-cyber-crime-botmaster.

[77] "Creators of SpyEye Banking Trojan Sentenced to 24 Years in Prison," *Tech Times* (April 23, 2016). http://www.techtimes.com/articles/152810/20160423/creators-of-spyeye-banking-trojan-sentenced-to-24-years-in-prison.htm.

[78] Kim Zetter, "Ukrainian Carding King 'Maksik' Was Lured to Arrest," Wired (July 28, 2010). https://www.wired.com/2010/07/maksik-lured-to-arrest/.

Operation Wellspring Expands to Other Jurisdictions

Following the success of the Wellspring pilot program in Utah, the FBI decided to expand Operation Wellspring to several other locations. As of November 2016, there are nine additional sites that participate in the partnership—San Diego, New York, Buffalo, Albany, Phoenix, New Orleans, Oklahoma City, Knoxville, and Kansas City, Missouri. This participation gives state and local law enforcement agencies in those cities access to FBI databases, training, and case referrals in the form of packets from IC3.

Many of the sites operate in a fashion similar to the Utah model in which investigators from state law enforcement agencies are stationed at FBI field offices. The next sections of this report describe the San Diego and New York cyber task forces.

Incorporating Operation Wellspring into an Existing State-Led Cyber Investigative Team: The San Diego CATCH Team

In San Diego, federal, state, and local partners all participate in an Operation Wellspring model based on a previously established cooperative effort, the Computer and Technology High-Tech Response Team (CATCH). Unlike other Wellspring programs that are housed in a federal agency, the CATCH team is housed and led by the San Diego County District Attorney's Office. The team has been in existence since 2000 when it was established through a grant from the Governor's Office. Incorporating Operation Wellspring allows the CATCH team to have access to FBI databases and receive packets from IC3. Partners include representatives from local prosecutors' offices, police departments, sheriffs' offices, the California Department of Motor Vehicles, and probation and parole agencies.[79] The FBI and U.S. Postal Inspection Service embed investigators in the state-run task force. Since 2011, the CATCH team is no longer funded by a state grant but rather has a direct appropriation from the California legislature as one of five cyber task forces operating in the state.

The CATCH team has experienced many of the same benefits as Operation Wellspring in Utah. Like the Utah program, the CATCH team can deconflict cases where there might otherwise be duplicative investigations among agencies by virtue of their cooperation. The FBI also provides training to the state and local investigators on the CATCH team on the technical aspects of high-tech cases. This investment is a significant benefit, because cyber issues evolve quickly.

Investigators also credit the joint effort between the FBI and state and local investigators for providing the type of multi-jurisdictional, coordinated response that is required to address the unique nature of cyber crime. In one successful example, the team handled a computer-enabled fraud case where the perpetrator used online advertising to rent a beachfront property to several victims at once. The FBI referred the case to the CATCH team because the financial losses did not meet the FBI's threshold for

[79] The CATCH team has included representatives from the following agencies: California Department of Justice, California State Parole, California Department of Motor Vehicles, Carlsbad Police Department, FBI, Imperial County District Attorney's Office, Riverside County District Attorney's Office, Riverside County Sheriff's Department, San Diego County District Attorney's Office, San Diego County Probation, San Diego County Sheriff's Department, San Diego Police Department, and the U.S. Postal Inspection Service.

investigation. The CATCH team was able to prosecute the perpetrator and obtain restitution for the victims for about 90 percent of their financial losses.

Even though the CATCH team focuses on high-tech and computer-enabled crime, the group looks for the most appropriate avenue for prosecution. Prosecuting high-tech crimes under traditional statutes may enable higher penalties. A network intrusion that monetizes data, for example, might simply be charged as grand theft or larceny.

Because multiple law enforcement agencies are involved in CATCH, decisions must be made about which agency will take a given case to prosecute. Generally, the decision depends on which agency is considered most likely to successfully obtain a conviction. In one instance, the team located a suspect who had stalked a victim online. However, the police did not have probable cause to arrest the individual because there was no direct contact between the victim and suspect. Working with the FBI, the CATCH team was able to hand the case to a federal prosecutor who could make an arrest under statutes related to travelling across state lines with intent to injure or harass.[80] The lead CATCH investigator from the San Diego County Sheriff's Office stated, "We like to see where we can get the biggest bang for our buck, i.e., who will have a better shot at prosecution."

The CATCH team has also confronted the challenge of measuring its successes. Similar to the measures that Utah DPS uses, the CATCH team keeps track of the following metrics in order to report on its progress:

- Number of tips/leads investigated
- Number of cases filed
- Number of victims involved in the cases filed
- Number of arrests
- Number of convictions obtained
- Aggregate monetary loss suffered by the victims it assists

As in many other cyber crime units, though, the number of tips or leads that investigators receive and assess far outweighs how many become filed cases.

Because the CATCH team has been established for 16 years, it has also developed strong relationships with private-sectors partners. Some of the crime victims served by CATCH are "repeat customers"—private-sector companies, government agencies, universities, and other organizations that have experienced multiple breaches of their data systems and which feel comfortable reporting high-tech crimes because of earlier positive experiences with CATCH team members. Officials want to reduce the stigma associated with breaches of data systems, because even good systems can be hacked. Reducing the stigma will result in increased reporting of breaches, which will help others learn about current threats and countermeasures. The team participates in a regional Securing Our E-City Initiative with industry partners, which builds a relationship between police and private-sector partners to build cyber resilience

[80] The Interstate Stalking Act, 18 U.S.C. § 2261A (1996). https://www.law.cornell.edu/uscode/text/18/2261A.

and a safe digital community in San Diego. CATCH also conducts extensive outreach to private companies in the area.

Operation Wellspring With Local Law Enforcement at the Helm: The FBI Cyber Task Force (New York City)

Police executives who are considering whether to adopt an Operation Wellspring model should understand that the program need not be led by a state agency. In New York City, multiple agencies participate alongside the FBI, including the New York City Police Department (NYPD). Many NYPD cyber crime investigators are embedded in the FBI New York Field Office, divided into subsections based on the type of cyber crime. Altogether, there are multiple task force cyber squads that investigate national security (terrorist-sponsored and state-sponsored), computer intrusions, hacktivism, dark web investigations, and cyber crimes against the financial sector.

> **"Cyber crime knows no geographical boundaries and expands the exposure to victims throughout the world. This task force extends the reach of law enforcement to help identify, pursue, and prosecute those who commit cyber crime, wherever they may be."**[81]
>
> ***—Former Commissioner William Bratton, New York City Police Department***

Operation Wellspring in New York operates out of the FBI's Cyber Crimes Task Force, whose six full-time NYPD investigators are a part of the NYPD's Grand Larceny Division. The FBI established the Financial Cyber Crimes Task Force in 2014 in conjunction with the NYPD and the Metropolitan Transit Authority (MTA). Now, the task force has expanded to include partners from the Nassau County Police Department, the Suffolk County Police Department, and the Sea Gate Police Department. The squad addresses cyber crime targeted at the financial sector like ATM skimming and fraud. At this time, approximately one quarter of the task force's referrals come from IC3, meaning tips and complaints the public submits online at ic3.gov.

Now that the task force has two years' experience working together, NYPD investigators and FBI agents are able to identify ways in which working together has served as a "force multiplier." The FBI agents tend to have extensive technical subject matter experience and the NYPD detectives have extensive fraud investigative experience. Partnering has created a dynamic where officers and agents are learning from and training each other. The FBI agents can assist NYPD officers with complicated technical issues like network intrusions or digital evidence extraction. Detectives can assist agents with their major fraud investigation and city-wide capability network.

[81] https://www.fbi.gov/newyork/press-releases/2014/fbi-new-york-announces-newly-formed-cyber-task-force-with-nypd-and-mta.

"The whole idea is to combine local insight with a global reach."

—Deputy Chief Joseph Dowling, NYPD Grand Larceny Division

The NYPD also possesses an extensive knowledge of the dynamics on the ground. In New York, criminal organizations that are active in traditional crimes are increasingly venturing into cyberspace.[82] Gangs are recognizing that computer-enabled financial crimes carry smaller penalties than other gang-related crimes such as narcotics sales. Cyber crime also is seen as having a lower risk of identification and enormous potential for financial gain. The NYPD's experience and knowledge of these criminal organizations give the FBI the local insight that can bolster investigations. Employing an intelligence-led policing model, the task force aims to identify leaders of criminal rings that commit cyber financial crimes and then capitalize on federal partnerships to impose more serious criminal penalties. For example, in federal court, aggravated identity theft carries a mandatory minimum prison term of two years.[83]

In terms of measuring success, NYPD agreed that clearance rates should not be the sole performance measure for cyber financial crimes. The task force is keeping track of investigators' caseloads, including the number of cases assigned, in a weighted system that assigns more credit to time-consuming or complicated cases (for example, cases that result in the identification of a foreign perpetrator). Investigators also keep track of specific benchmarks that they reach throughout the course of their investigation—identifying IP addresses, filing search warrants, or successfully obtaining legal process, for example. Operation Wellspring in New York also tracks the amount of funds it recovers, which is estimated to be in the tens of millions in the past two years.

Partnerships with the Private Sector

Lesson Learned: Building Trust With the Private Sector Is Crucial to Understanding Cyber Crime

One of the unique facets of cyber crime is that cyber crime investigators share a close relationship with cyber intelligence analysts. It is essential for effective cyber investigations to foster information sharing between the investigative and intelligence functions in an agency. Therefore, one key challenge for police executives is how to encourage information sharing and crime reporting among private-sector partners so that police intelligence officers can benefit from the wealth of expertise in the private sector and learn about the most current trends in cyber attacks that affect the private sector. The FBI estimates that approximately 80 percent of high-tech crime discovered by network administrators and company

[82] John Annese and Shayna Jacobs, "Bloods-linked gang members charged with running $414G identity-theft ring," *New York Daily News* (April 27, 2016). http://www.nydailynews.com/new-york/nyc-crime/bloods-linked-gang-members-charged-414g-id-theft-ring-article-1.2615754.

[83] See 18 U.S. Code § 1028A, "Aggravated Identity Theft." https://www.law.cornell.edu/uscode/text/18/1028A.

executives is never reported to law enforcement.[84] Certainly, there is a clear business reason why reporting may not happen, as companies' reputation and profits may depend greatly on their ability to appear impenetrable. Companies too often absorb losses quietly in what may seem the best approach, at least in the short term.

The FBI is conducting a massive outreach effort to encourage information sharing and engage private-sector companies throughout the country on cyber crime issues. The FBI established InfraGard in 1996, a partnership between the bureau and private partners (particularly in sectors that involve homeland security or critical infrastructure), which is dedicated to sharing information and intelligence on cyber attacks.

The FBI shares information with private-sector partners through a variety of methods: public service announcements posted on the FBI's website, technically oriented FBI Liaison Alert System (FLASH) messages, and Private Industry Notifications (PINs) that provide unclassified risk assessments to subscribing industry partners. The FBI has also incorporated private-sector partners into the National Cyber Forensics and Training Alliance (NCFTA), a nonprofit organization dedicated to identifying and neutralizing global cyber crime threats. The FBI has also provided a 24-hour resource center for private companies called "CyWatch" that serves as a command center for cyber intrusion prevention and response.

Following the Sony Pictures Entertainment hack in 2014, the FBI established a precedent for how to work with the private sector following a cyber attack. Sony was able to set the terms of its information sharing, including reasonable limitations on what the FBI accessed. The FBI now employs the "Sony Model" for its cyber investigations, which includes an emphasis on the victim, establishment of trust, a single point of contact from the government, mutual information sharing, and the embedding of agents at the company. Overall, the FBI recognizes that investigators need to take a victim-centered approach about cyber crime and treat companies as victims.[85]

State and local agencies that investigate cyber crime must also reach out to private-sector partners and build trust to the point where business people feel comfortable reporting crimes and sharing information. It helps FBI investigators to obtain information about the types of cyber attacks that network administrators are seeing and how criminals are able to breach networks. This helps the FBI aggregate and prioritize cases. Law enforcement agencies will never obtain a comprehensive understanding of the

[84] James Trainor, "Confronting Cyber Threats: Cybersecurity from the FBI's Perspective," The Massachusetts Attorney General's National Cyber Crime Conference, Norwood, MA, Keynote Address (April 25, 2016).

[85] A "victim-centered" approach is often discussed in the context of sex crimes, human trafficking, and other offenses involving special victims. For example, in the context of human trafficking, DHS defines a victim-centered approach as one that places equal emphasis on identification and stabilization of victims, with particular focus on ensuring that police do not retraumatize them. *See* https://www.dhs.gov/blue-campaign/victim-centered-approach. Applying this concept to cyber investigations, police are recognizing the need to identify victims of cyber crime, help ensure their financial wellbeing and bolster their cybersecurity, and minimize any potential negative impact the investigation may have on victims.

facets and magnitude of the cyber crime landscape without the experiences and insight of private-sector partners.

Promising Practice: Build State Information-Sharing Initiatives that Allow Private-Sector Partners to Decide the Terms of Their Involvement

Recognizing the importance of working with the private sector within Utah, Operation Wellspring has made outreach and relationship building a priority. For its computer-enabled fraud cases, Utah's Department of Public Safety has reached out to online auction websites and other systems that criminals use to commit fraud, such as eBay and local online classified advertisers, to make them aware of recent trends in computer-enabled fraud. Major Brian Redd, Director of the Utah State Bureau of Investigation, said "that traditionally, there is a belief among police investigators that while an investigation is ongoing, the information pertaining to it should stay close with the detective." Major Redd is working with his investigators and intelligence analysts to identify how to get as much information as possible to private partners, while still protecting information that cannot be shared, or, in some cases, sharing documents that have been partially redacted in order to protect identities.

Importantly, DPS participates in federal information-sharing initiatives like the FBI's InfraGard. It also became clear that law enforcement agencies in Utah needed an information-sharing effort across the state. So, DPS Commissioner Squires tasked the Statewide Information and Analysis Center (SIAC) with strengthening the Cyber Intelligence Liaison Officer (ILO) network. Cyber ILO partners are personnel with technical expertise from both public and private organizations. One reason the Cyber ILO was created was to better inform stakeholders where to report cyber incidents. For example, the Cyber ILO program helps spread awareness about the Internet Crime Complaint Center (IC3) as the main point of contact for the public to report cyber crimes (for more information on IC3, see previous Sidebar "*The Internet Crime Complaint Center (IC3)").*

Another reason to partner with the private sector is to gain access to its knowledge and experience. Cyber incidents such as malware intrusions have existed for many years, and private companies have been dealing with network intrusions for decades. This experience in cyber security can be invaluable to law enforcement as it integrates the cyber intelligence and investigative functions of its agencies. DPS is building trust with cyber professionals in the private sector in order to increase crime reporting. Commissioner Squires has developed a strategy to build trust over the long term with a tiered participation system. Private companies decide the extent of their involvement in the Utah Statewide Cyber Intelligence Network (USCIN) on a voluntary basis. The criterion for participation is that partners must be IT administrators for an organization with ties to Utah. Initially, private-sector partners can sign onto the lowest tier where they simply elect to receive cyber bulletins from SIAC. The second level of involvement allows partners to anonymously share information concerning cyber threats or attacks. The third tier allows ILOs to share the specifics of a cyber attack against their companies with other members of the network. The SIAC is also considering the potential for creating subcommittees in various sectors of private businesses such as retail businesses, construction, or real estate once there is a critical mass of ILO partners representing various industries.

"Success in the Intelligence Liaison Officer network would be receiving raw intelligence reports from our partners, and breaking down barriers to create relationships and partnerships."

—Commissioner Keith Squires, Utah Department of Public Safety

Promising Practice: Housing a Private-Sector Partner at the Fusion Center Is an Effective Way to Support Information Sharing

In order to understand the threats facing the private sector, the Utah DPS is encouraging private-sector agencies to identify an employee who can participate in SIAC on a full-time basis. This employee will work with the cyber intelligence analyst in real time to analyze threats and enhance the state's cybersecurity network and response to attacks. The idea of including private-sector employees in fusion centers is consistent with the federal government's Fusion Center Initiative, which integrates a private sector component.[86] The goal is to merge the knowledge, data, and insights of the private sector with those of law enforcement agencies, thereby strengthening both sides' intelligence networks.

DPS is in the process of vetting candidates from the private sector to serve in a pilot program. Funding for private sector personnel would come from the private-sector partner. In order to house a private-sector employee at SIAC full time, there are several procedures that DPS must establish to comply with federal Department of Homeland Security (DHS) requirements. The candidate must obtain or already possess a TS-SCI level clearance in order to access government information. DPS is implementing a Memorandum of Understanding with nondisclosure components to address private-sector partner concerns, particularly the unauthorized release of propriety or sensitive information and the potential for private-sector involvement in investigations that could result in regulatory penalties.

[86] The Department of Justice's Global Sharing Initiative and the Department of Homeland Security, Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era (2008). http://it.ojp.gov/documents/d/fusion_center_guidelines.pdf.

Integrating Cyber Resilience into Existing Public Safety Capabilities

A Picture of the Threat

In December 2015, a group of coordinated hackers broke into the cyber network of a Ukrainian utility company's power control center, shutting down dozens of power substations and backup systems within a span of 30 minutes. This action left more than 230,000 Ukrainian residents in the western part of the country without power on December 23, 2015 for several hours.[87] In order to maximize the impact of the outage, hackers also coordinated a large telephone denial-of-service (TDoS) attack against the utility company's phone system. A massive volume of bogus calls overwhelmed the system and prevented customers from contacting the electrical utility.[88]

Experts say that the attack had less of an impact than a similar attack might have had in the United States. The Ukraine utility used old technology that is not fully wired that allowed workers to manually switch circuit breakers back on to restore power.[89] In the United States, many electrical utility systems do not have such manual backup capabilities. The targeted concentration of the attack led cyber experts to speculate that the attack was politically motivated and was intended to send a message.[90] Careful investigation after the attack revealed that hackers had penetrated the power grid's cyber network and controlled portions of it for 6 months before the attack occurred, coordinating an extensive strategy to maximize their synchronized assault through extensive reconnaissance.[91]

This attack was not unexpected. Officials warn that the U.S. power grid is not sufficiently prepared to thwart potential hackers and that hackers from China, Russia, and Iran may already be inside the United States' system, capable of attacking and deterred only by the fear of retaliation by the United States.[92] Notably, officials are increasingly becoming concerned about the potential for a cyber attack on a nuclear facility, with one reportedly happening in the past few years.[93]

---

[87] Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired Magazine* (March 3, 2016). https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.
[88] Kim Zetter, "Everything We Know About Ukraine's Power Plant Hack," *Wired Magazine* (January 20, 2016). https://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/.
[89] David E. Sanger, "Utilities Cautioned About Potential for a Cyberattack After Ukraine's," *The New York Times* (February 29, 2016). http://www.nytimes.com/2016/03/01/us/politics/utilities-cautioned-about-potential-for-a-cyberattack-after-ukraines.html.
[90] *Ibid.*
[91] Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired Magazine* (March 3, 2016). https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.
[92] Cory Bennett, "Congress struggles to secure nation's power grid," The Hill (November 26, 2015). http://thehill.com/policy/cybersecurity/261310-congress-struggles-to-secure-power-grid.
[93] Andrea Shalal, "IAEA Chief: Nuclear power plant was disrupted by cyber attack," Reuters (October 10, 2016). http://mobile.reuters.com/article/idUSKCN12A1OC.

In addition, there have been unsuccessful cyber attacks on critical infrastructure in the United States. In March 2016, the U.S. Attorney from the Southern District of New York indicted seven Iranian nationals who allegedly worked for the country's Islamic Revolutionary Guard Corps for a 176-day distributed denial of service (DDoS) that attempted to take control of a small dam in New York State.[94] This type of an event can be termed a "cyber disruption." A response to a cyber disruption requires a coordinated effort among multiple types of partners within the private sector and government. For example, a disruption in the functioning of some key infrastructure or delivery of some utility such as distributed electrical power, water, or natural gas, interruption in waste water treatment, loss of telecommunications or Internet services, and interruption in wireless service or radio communications may trigger an emergency response. As the event is being evaluated by emergency management, it may be discovered that the underlying cause is, in fact, a cyber disruption.[95] As a result, communication between emergency management personnel and cyber security professionals is essential for de-confliction and creating a coordinated response to the disruption with implications for both areas.

The National Association of State Chief Information Officers (NASCIO) has developed the Cyber Disruption Response Planning Guide that outlines an integrated operating discipline describing necessary actions based on an event threat level. The guide presents the need for established governance that includes the governor's office, the state chief information security officer (CISO), emergency management, National Guard, state police, fusion centers, and industry partners.[96]

Attempts to use cyber attacks as international weapons have the potential to dramatically change the landscape of foreign policy and international relations. In 2009, a virus known as "Stuxnet," which has been called the world's first "cyber missile,"[97]attacked and destroyed a fifth of the nuclear centrifuges used to enrich uranium in Iran, setting a precedent for current modern attacks.[98] Although the attack has never been officially attributed to the United States, experts believe it was the result of a joint American-Israeli effort.[99] Stuxnet was introduced to the Iranian Natanz nuclear facility's network through a corrupt thumb drive by a worker in the plant. The Stuxnet worm secretly recorded what normal operations at Natanz looked like and played those readings back to plant operators so that operations would appear normal, but at the same time, the worm took control of the centrifuges, making them spin too fast so that they would be damaged or destroyed. Following this attack, experts believe that an increasing reliance on

---

[94] David E. Sanger, "U.S. Indicts 7 Iranian in Cyberattacks on Banks and a Dam," *New York Times* (March 24, 2016). http://www.nytimes.com/2016/03/25/world/middleeast/us-indicts-iranians-in-cyberattacks-on-banks-and-a-dam.html.

[95] NASCIO, *Cyber Disruption Response Planning Guide* (April 2016) p. 72. Retrieved on March 6, 2017 from http://www.nascio.org/Publications/ArtMID/485/ArticleID/358/Cyber-Disruption-Response-Planning-Guide.

[96] *Ibid.*

[97] Mark Clayton, "How Stuxnet cyber weapon targeted Iran nuclear plant," *Christian Science Monitor* (November 16, 2010). http://www.csmonitor.com/USA/2010/1116/How-Stuxnet-cyber-weapon-targeted-Iran-nuclear-plant.

[98] Michael B. Kelly, "The Stuxnet Attack on Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought," Business Insider (Nov. 20, 2013). http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11.

[99] William J. Broad, John Markoff, and David E. Sanger, "Israeli Test on Worm Called crucial in Iran Nuclear Delay," *New York Times* (January 15, 2011). http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all&_r=0 .

cyber attacks as a military weapon have, as commented Ralph Langner, "changed global military strategy in the 21st Century."[100]

Incorporating Cyber Concerns into the Existing Homeland Security Framework in Utah

Based on Guidance from the Federal Government

Throughout the federal government there are a variety of entities and initiatives that provide guidance to state and local law enforcement agencies on how to build resiliency to cyber attacks on Critical Infrastructure and Key Resources (CIKR). For example, the Department of Justice's (DOJ's) Global Justice Information Sharing Initiative ("Global") in 2015 drafted a set of specific guidelines for state and major urban area fusion centers on how to add a cyber component[101] in line with DOJ's current general guidelines for fusion centers.[102]

The National Institute of Standards and Technology (NIST) created a voluntary cyber framework under the direction of Executive Order 13636 to reduce cyber risks to CIKR; the framework can be used to assist state and local governments and private-sector partners.[103] NIST is the federal technology agency that works with private-sector partners to develop and apply technological standards. NIST's Framework for Improving Critical Infrastructure Cybersecurity[104] helps non-government owners of critical infrastructure to ensure that their cyber security efforts consistently reflect the latest best practices throughout the country.

The Department of Homeland Security (DHS) launched the Critical Infrastructure Cyber Community (C^3, pronounced "C cubed") Voluntary Program[105] in 2014 to provide support to owners of critical infrastructure and their partners in bolstering resiliency to cyber risk. It constitutes the coordination point within the federal government for helping critical infrastructure owners and operators to voluntarily improve their cyber risk management. The mission of C^3 is to: "1) support industry in increasing its cyber

[100] Ralph Langner, "Stuxnet's Secret Twin," *Foreign Policy* (November 19, 2013). http://foreignpolicy.com/2013/11/19/stuxnets-secret-twin/.
[101] Global Justice Information Sharing Initiative, Cyber Integration for Fusion Centers: An Appendix to the Baseline Capabilities for State and Major Urban Area Fusion Centers (2015) file:///C:/Users/mbrunner/Downloads/Cyber%20Integration%20for%20Fusion%20Centers.pdf.
[102] See Global Justice Information Sharing Initiative, Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era (2006) available at https://it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf and Global Justice Information Sharing Initiative, Baseline Capabilities for State and Major Urban Area Fusion Centers (2008) available at https://www.it.ojp.gov/documents/d/baseline%20capabilities%20for%20state%20and%20major%20urban%20area%20fusion%20centers.pdf.
[103] http://www.nist.gov/cyberframework/.
[104] https://www.nist.gov/cyberframework.
[105] https://www.dhs.gov/ccubedvp.

resilience; 2) increase awareness and use of [the NIST] Framework; and 3) encourage organizations to manage cyber security as part of an all hazards approach to enterprise risk management."[106]

DHS also manages the National Cybersecurity and Communications Integration Center (NCCIC),[107] which provides around-the-clock cyber situational awareness and incident response. NCCIC is the management center that integrates cyber and communications for the federal government, intelligence community, and private sector. Through its United States Computer Emergency Readiness Team (US-CERT) and Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), NCCIC provides private-sector stakeholders with actionable cyber security information and technical support to restore services and mitigate incidents.

DHS also operates the Protective Security Advisor (PSA) Program,[108] which assists state and local government entities responsible for protecting CIKR by providing a liaison to support and coordinate their efforts. PSAs can: 1) provide direct technical assistance to CIKR specialists in their states on resiliency planning; 2) help build bridges between private partners and state and local law enforcement; 3) serve as liaisons between communities and the federal government following an incident that affects critical infrastructure; and 4) provide training on CIKR protection to private-sector partners.

The programs cited above are just a few examples of the many efforts across the federal government. There are also significant contributions from groups like the Criminal Intelligence Coordinating Council, Multi-State Information Sharing & Analysis Center, Program Manager for the Information Sharing Environment, and many others. Across the country, states, regions, and cities have begun to develop coordinated cyber security efforts in response to potential cyber threats.[109]

Commissioner Squires said he understands the importance of integrating cyber concerns into the current state emergency management framework, and has made this his top priority for the next phase of the Utah Model. This requires not only bolstering cyber security to prevent potential attacks but also writing a detailed response and recovery plan.

The cyber resilience component is part of the DPS, Department of Emergency Management (DEM), and SIAC's larger initiative to protect CIKR with its Utah Whole Community Infrastructure Resilience Program, in line with DOJ's Global Justice Information Sharing Initiative's Cyber Integration for Fusion Centers.[110] The program's coordinator, the critical infrastructure protection coordinator housed in DEM, is responsible for ensuring compliance with NIST standards and liaising with ICS-CERT, for example. A large

---

[106] https://www.dhs.gov/sites/default/files/publications/C3%20Voluntary%20Program%20Informational%20Graphic.pdf.

[107] https://www.dhs.gov/national-cybersecurity-and-communications-integration-center#wcm-survey-target-id.

[108] https://www.dhs.gov/protective-security-advisors.

[109] For example, the City of Los Angeles recently built a state-of-the-art Integrated Security Operations Center (ISOC) to coordinate citywide cybersecurity efforts and incident response. See Tara Seals, "Inside the City of LA's ISOC Project," *Infosecurity Magazine* (October 13, 2015). https://www.infosecurity-magazine.com/news/inside-the-city-of-las-isoc-project/.

[110] Global Justice Information Sharing Initiative, Cyber Integration for Fusion Centers (2015). https://it.ojp.gov/GIST/178/Cyber-Integration-for-Fusion-Centers--An-Appendix-to-the-Baseline-Capabilities-for-State-and-Major-Urban-Area-Fusion-Centers.

part of the work is outreach and building trust between private-sector and emergency management officials to ensure the recovery of CIKR after critical incidents. Utah also has a Critical Infrastructure Prioritization tool that assigns point values to CIKR based on their potential impact on Utah residents. Through these efforts, DEM and SIAC can connect local cyber security professionals to federal government resources.

State Governments' Role in Enhancing Cyber Security: A Spotlight on the Role of Governors and the National Governors Association

In recent years, states have been making large strides toward enhancing their cyber resilience. States are looking to leaders in state-level cyber security like Michigan and Utah for guidance and at the leadership of Governor Rick Snyder and Governor Gary Herbert.

In addition, the National Governors Association (NGA), a bipartisan organization whose mission is to share best practices and develop policy solutions for state government, considers state-level cyber security a top priority moving forward. The organization has been a leader in the field, both in the 2012 creation of its Resource Center for State Cybersecurity[111]—to give governors information on cyber risk—and in holding national cyber security summits for state leaders.

"Our main goal right now is to help states focus on developing comprehensive cyber security strategies based on personalized risk assessments," said Tim Blute, NGA Program Director for the Homeland Security & Public Safety Division. In essence, each state needs to take an individual look at reducing the risks particular to their locality and anticipate all the ways that cyber threats may impact their agencies, private-sector partners, and constituents. The goal is for every state—regardless of how mature their cyber security frameworks may be—to move forward toward increased cyber resilience.

NGA's current work is now centered on two complementary initiatives:

- NGA's Meet the Threat Initiative[112] is intended to push states toward doubling down on prior cyber security work while challenging state leaders to push toward a broader understanding of resilience. For example, rather than narrowly focusing on cyber threats' impact on critical infrastructure, NGA is encouraging states to tackle cyber security in even more sectors (e.g., health care or education). NGA's overall hope is to raise awareness on how cyber threats impact states. "The initiative has the potential to shape the nation's response to the growing cyber threats we face by underscoring the critical role state leaders play in securing the cyber environment," said Governor Terry McAuliffe of Virginia, Chair of the NGA.
- NGA is also conducting intense technical assistance through its Policy Academy. As of the beginning of 2017, NGA is working with five different states to enhance their disruption response plans and help them resolve critical incident planning challenges.

[111] https://www.nga.org/cms/statecyber.
[112] https://ci.nga.org/cms/home/ci1617/index.html.

Promising Practice: Creating a Specific Cyber Incident Response Plan and Incorporating Cyber Incidents into Existing Plans

To ensure that cyber crime prevention and enforcement were a part of Utah's overall Emergency Management Plan, Commissioner Squires established a working group in Utah's Division of Emergency Management (DEM), which operates the Utah Emergency Operations Centers. The working group meets monthly to work on integrating cyber concerns into the State of Utah's emergency management structure. The working group also created a subcommittee to draft a Cyber Incident Response Plan in the event of a cyber attack that could affect critical infrastructure in the state. The subcommittee includes the cyber intelligence analyst from SIAC, the critical infrastructure protection coordinator, DHS's protective security advisor, the Utah DEM's planning section manager, and a representative of the Department of Technology Services (DTS). The subcommittee connects personnel with expertise in emergency management and continuation of operations planning with those who have technical expertise in cyber issues (SIAC's cyber analyst, and DTS personnel).

The Cyber Incident Response Plan, informally known as the "Cyber Annex," was developed by this subcommittee, based on a toolkit that DHS provided. The subcommittee relied on the expertise of DHS's protective security advisor and also reviewed cyber incident plans from other states throughout the country. The plan details actions that the Utah state government should take following a cyber critical incident. In the past, Utah state government officials said they thought that if there was a major cyber incident, DTS would simply handle the problem; they were unaware that they would need to take proactive steps at their own agency to report and remediate in the event of an attack.

Commissioner Squires hopes that the Cyber Annex also will help local governments think about cyber incident planning and educate private-sector companies that may not yet be focused on cyber issues. As a part of the planning work, the group held a large meeting with critical members of the private sector to brief them on the planning effort. Some private-sector companies that could be hurt financially by any disruption in critical infrastructure were willing to make financial contributions to the planning effort. (The final plan is available in Appendix A.) DEM plans to also integrate cyber concerns into its existing Emergency Operations Plan and Continuation of Operations Plan.

In advance of any cyber event, a collaborative network must be built that clearly delineates the role of each partner. Important members of any state cyber disruption network include regional and national organizations that are already in place to facilitate situational awareness and information exchange with respect to cyber issues. These include:

- The National Cybersecurity and Communications Integration Center (NCCIC)
- The Multi-State Information Sharing & Analysis Center (MS-ISAC)
- State-specific Information Sharing Analysis Center ([state]–ISAC)
- The United States Computer Emergency Readiness Team (US-CERT)
- The National Fusion Center Association Cyber Threat Intelligence Subcommittee (NFCA–CTI)
- The Information Sharing and Analysis Organization (ISAO)

Promising Practice: Test the Effectiveness of a Cyber Incident Response Plan through Multi-Agency Tabletop Exercises

The major purpose of the Cyber Annex is to assign roles and responsibilities for responding to a cyber attack against Utah state networks. In order for the subcommittee to assess whether the plan worked and assigned responsibilities effectively, it needed to conduct a training exercise to test incident response in a controlled environment. The subcommittee specifically wanted to test protocols for reporting an incident to the Utah Emergency Operations Center and ways to preserve forensic evidence (e.g., not erasing computer hard drives), so that DPS can investigate cyber attacks.

In February 2016, the Utah state government had its first tabletop exercise to simulate responses to a cyber incident. The subcommittee started with requesting technical assistance from DHS, which had members thinking about the potential impact of a cyber attack on the state and how to start the cyber preparedness process. The subcommittee decided the best course of action would be to plan an initial tabletop exercise with one government agency.

Because of the sensitivity of protected health information (PHI) and the increase in cyber attacks on agencies that handle it, the Utah Department of Health volunteered to be the pilot agency. The tabletop simulated an attack on a laboratory that released a toxic organic sample into the air after a hack into the lab's computer-controlled HVAC system. Personnel had to first determine that it was, in fact, a cyber attack, and then put in place the procedure for remediating the incident. The tabletop in February resulted in a debrief that compiled a list of lessons learned that improved the protocols in the Cyber Annex.

In May 2016, the subcommittee oversaw a tabletop exercise that affected multiple sectors and therefore required a multi-agency response. The committee integrated the lessons from these training exercises into the Cyber Annex document. In the future, Commissioner Squires wants to organize a tabletop exercise that also involves private-sector partners. The subcommittee plans to do a multi-agency Cyber

Incident Tabletop every year to scrutinize the Cyber Annex and prepare personnel. The trainings will ensure that personnel in the Utah state government will know how to handle a critical cyber incident affecting state infrastructure, and they can serve as a model for local government and private-sector partners.

[Page Intentionally Blank]

Summary and Conclusion

Faced with the growing threat of cyber crime, local and state police agencies have recognized that it is not enough to leave cyber resiliency and investigations of cyber crime to the federal government. Police executives throughout the country will find the experiences of the Utah Department of Public Safety and other Operation Wellspring Model programs instructive as they seek to build or enhance their own programs.

Cyber crime deterrence programs require all the elements of other proactive law enforcement programs: leadership, legislative support, funding, training, and experience. Cyber investigations and prevention of cyber crime also pose special challenges to law enforcement agencies. The following is a summary of the challenges, promising practices, and lessons learned for police executives as they address this exponentially growing area.

Why Invest in a Cyber Program?

It is crucial for state and local police agencies to invest in cyber programs. Cyber crime—both high-tech crime (where computer networks are targets) and Internet-enabled crime (where a computer is used as a tool)—is expanding rapidly throughout the world. From the standpoint of a criminal offender, cyber crime is a relatively low risk type of crime that has the potential for enormous rewards. Until police agencies become adept at preventing and investigating cyber crime, there may not be significant deterrents to thwart cyber crime relative to other types of crime.

Police agencies must see addressing cyber crime as a part of their mission. State and local law enforcement agencies may perceive the FBI as the agency best equipped to investigate cyber crime. However, it is crucial to understand that no agency can fight this type of crime alone. The FBI needs assistance from its state and local partners, just as local agencies need the FBI's assistance.

Some police executives may be hesitant to expend resources on cyber crime as opposed to other priorities, because much of cyber crime is property crime, not violent crime. That view does not account for the profound impact that cyber crime can have on an individual victim or on the economy in the aggregate. Police agencies need to see it as their mission to step in and protect individuals and businesses from this growing threat. And certain types of cyber crime such as swatting can result in physical injuries or death to victims.

Furthermore, cyber crime is not entirely about thefts of money from bank and credit card accounts. Cyber crime also involves threats to critical infrastructure such as electric companies and other public utilities and threats to national security.

Governments and police agencies are increasingly victims themselves. The increase in cyber attacks on state and local governments, including police agencies, is another reason why police executives must invest in creating robust cyber programs. Government agencies are ripe targets for cyber criminals because of the sensitive information with which they are entrusted. Being able to hack or steal data from

a government agency can embolden hacktivists or those looking to do harm to the United States. There has been an increase in ransomware, hacktivism, and swatting attacks against government employees, including police. In order for state and local governments to operate effectively, police agencies must be committed to investigating all attacks against governmental bodies.

How to Build a Cyber Program

Define "Cyber Crime" and Determine the Scope of a Program. The first step for state and local police agencies interested in creating or supporting a cyber crime unit is determining what crimes they will address. Will the unit exclusively look into high-tech crimes where computer networks are the target? This would include crimes like network intrusion, denial of service, and ransomware, or will the unit also tackle Internet-enabled crimes where computers are used as tools to effectuate the criminal activity?

While that distinction may seem clearly defined on the surface, investigators find that in practice those distinctions can begin to blur. For example, a tech support scam that targets elderly victims may appear on the surface to simply be computer-enabled fraud. But if the fraud followed a breach that contained data on potential victims, then that may have originated from a high-tech crime. In Utah, the DPS Cyber Crimes Unit focuses its efforts on high-tech and computer-enabled crimes that have a critical mass of investigation related to the Internet—like the Nigerian Purchase Fraud case. Police executives must define the scope of their unit's activities, taking into account the complexities of cyber crimes, their resources, and other capabilities within their jurisdiction.

Prioritize Cyber Cases to Use Resources Effectively. Because of the enormous volume of cyber crime cases, police agencies must prioritize which incident leads they choose to investigate, and then which cases they open. Agencies often feel that these decisions amount to "triaging." For example, agencies often prioritize cases according to the size of the monetary losses. Intrusions on government computer systems also tend to be a high priority.

Furthermore, as a practical matter, the sophistication with which criminals can anonymize their activity on the Internet may mean that state police agencies may not be able to continue with many cases. Agencies need to put in place effective processes to vet tips and leads, and police executives must understand that a significant number of hours need to be dedicated to this vetting.

Educate Stakeholders to Maximize Resources. It is essential for police executives building a cyber program to work closely with their state government. Identifying influential advocates in state legislative bodies is an essential first step. Also, having dedicated funding to support cyber investigators is essential for the vitality and continued existence of any cyber efforts. Police agencies should educate their state and local government leaders on the growing cyber threat environment and the proliferation of cyber crime. Finally, updating the state criminal code to reflect the realities of cyber crime is essential for a victim-centered approach.

Understanding the Special Nature of Cyber Crime

Changing from "Reactive" to "Proactive" Requires a Change in Thinking. When state or local agencies decide to begin investigating cyber crime, they may need to retrain *all* personnel to change their ways of thinking about certain issues. For example, personnel need to be aware of protocols that make it possible to preserve evidence and conduct a digital forensic investigation (e.g., teaching officers to place a smartphone in airplane mode so that the data stored on it cannot be remotely deleted).

Cyber Investigations Can Require More Time Than Other Major Investigations. Cyber investigations can take a significant amount of time to investigate compared to other major crimes. As a primary matter, cyber crime units must spend a considerable amount of time vetting investigative leads in order to determine whether a case should be opened. Moreover, the elements of a cyber crime case often include information that must be obtained from private companies. And the process to obtain records through a subpoena or warrant can take months.

Defining Success Is Different for Cyber Units. Traditionally in policing, investigative units have been able to track and measure performance, defined as numbers of arrests or clearance rates. Because of the multitude of anonymity tools and the international nature of cyber crime, cyber investigations are less likely to result in an arrest. Therefore, police executives should understand the value of cyber investigations for other purposes. Investigations can be useful to a police agency if they result in actionable intelligence, the disruption of a criminal network, or the recovery of funds for a victim. Police agencies can use metrics to assess the performance of cyber crime units or individual investigators, but the metrics should not be the same as those for other units. Agencies should track performance measures like hours spent on investigations and vetting leads, monetary losses prevented and recovered, trainings and technical assistance provided to others, and intelligence products.

Cyber Units Have Unique Personnel and Management Issues. Because of the special nature of cyber crime investigations, there is also an impact on the investigators from a management perspective. Experts say that it can take 6 months or longer to become skilled in the technical aspects of high-tech investigations, and potentially 1 or 2 years for investigators to truly feel comfortable in their role. Professionals with cyber experience, in police agencies as well as the private sector, may also have high turnover because of their specialized skills in a growing field.

Law Enforcement Personnel Are Vulnerable to Personal Cyber Attacks. An important consideration for police executives is that their personnel may be subject to cyber attacks. Investigators and agency employees should make attempts to reduce their digital footprints. Executives should also prepare for the possibility that their personnel may get "doxed" or "swatted" (e.g., by securing funding for identity protection services).

Leveraging Partnerships

Partnering With the FBI Can Produce Many Benefits. One of the first lessons that state and local police executives have learned when building a cyber program is that no agency, not even the FBI, has the time and resources to address cyber crime on its own. Partnering together in joint task forces allows agencies

to take advantage of each other's strengths. For state and local agencies, partnering with the FBI enables a multi-jurisdictional reach that is needed for effective cyber investigations and prosecutions. FBI agents and local officers working together can learn from each other's technical and investigative experience. Operation Wellspring has given victims of computer-enabled fraud recourse that they did not have before, because their cases were too small for the FBI to investigate and prosecute. For jurisdictions considering implementing an Operation Wellspring partnership, they are advised to look well ahead for succession planning to account for changes in personnel due to the lengthy process for securing federal security clearances. Police executives should also understand that they need to secure their own funding for investigators when they sign onto Operation Wellspring.

Cases That Lead to International Actors Have Unique Challenges. There are additional challenges for state and local investigations when a cyber incident points to a perpetrator who is outside the United States. The potential for getting necessary evidence or effecting an arrest can vary widely, depending upon which country is involved. Formal procedures and going through the FBI's legal attachés to use MLAT and extradition treaties can take significant amounts of time, and less formal information-sharing methods can be difficult. In some cases, investigations by state and local police agencies can end with arrests if the state and local agencies are willing to hand the cases over to other countries' justice systems. Police executives must be comfortable with cyber cases being prosecuted by whichever entity is most likely to obtain a conviction.

Partnerships with the Private Sector Are Essential for Having an Accurate Picture of the Cyber Landscape. Private companies that are victims of cyber crime often neglect to report the incidents, in some cases because the incidents could produce unfavorable publicity. But there are some indications that companies are becoming less willing to view cyber crime as a "cost of doing business." For police agencies, increasing information sharing with the private sector is an essential step for cyber intelligence gathering and informed investigations. State and local police agencies have started to build networks with private-sector organizations. Outreach is a crucial component of any robust cyber program to make the technical experts and IT professionals within an agency's jurisdiction aware of the benefits of working together. One promising practice has been for police to allow a tiered system of voluntary information sharing in which private-sector partners can choose whether to merely receive information, share information anonymously, or allow other partners to know the full details of cyber attacks on their networks. State and major urban area fusion centers are also exploring parameters for allowing private-sector partners to staff personnel full-time at the fusion centers in order to gain further insight into the threat picture.

Incorporating Cyber Capabilities into an Existing Homeland Security Framework

Cyber Issues Must Be Considered When Planning for Critical Infrastructure Resilience. In the past year, a successful cyber attack against an electrical utility in Ukraine served as a wake-up call to law enforcement agencies around the world about the threat of cyber attacks on critical infrastructure. State and local agencies should integrate planning for recovery after cyber attacks as a part of their preparedness, including incorporating cyber issues into their emergency operations and continuation of operations planning.

Create a Cyber Incident Response Plan That Is Tested Through Tabletop Exercises. Law enforcement executives can take the lead in planning for a coordinated response in the event of a cyber critical incident. One essential task is to bring together a variety of experts—those who specialize in emergency management planning and those with technical cyber expertise—to draft a comprehensive Cyber Incident Response Plan. States should consider conducting multi-agency tabletop exercises to test the protocols and train personnel. Topics should include reporting procedures, remediation steps, and how to preserve forensic digital evidence for investigation.

Glossary of Terms and Names

Anonymous—Anonymous is a loosely associated group of hackers known for using cyber attacks on governments, businesses, and other institutions in order to draw attention to various social and political causes.[113]

Application log files—Application log files are detailed reports of a software application's history of activity. The data can include users' actions, system warnings, and errors.[114]

Bitcoin—Bitcoin is a digital currency and payment system that uses peer-to-peer technology rather than a central bank or intermediary authority. While there are legitimate uses for Bitcoin, it is a preferred currency for cyber criminals because of its decentralized and virtual nature.[115]

Cyber intelligence—Intelligence regarding threats posed to computer networks and systems. Often this intelligence is gathered through monitoring and analyzing cyberspace activity. This can include specific information on how a cyber attack was able to intrude a network, for example, or information on the tactics, techniques, and procedures of particular cyber criminals.[116]

Cyber Disruption—An event or effects from events that are likely to cause, or are causing, harm to critical functions and services across the public and private sectors by impairing the confidentiality, integrity, or availability of electronic information, information systems, services, or networks that provide direct information technology services or enabling and support capabilities for other services; and/or threaten public safety, undermine public confidence, have a negative effect on the state economy, or diminish the security posture of the state.[117]

Cyberspace—The globally connected network of computers is known collectively as "cyberspace."[118]

Botnet—a network of computers infected with malware (individually called "bots") used by hackers to disperse viruses and launch computer attacks. Botnets can consist of a few hundred bots to hundreds of thousands of bots, often without users being aware their computers are infected.[119] [120]

---

[113] Geneva Sands, "What to Know About the Worldwide Hacker Group 'Anonymous,'" *ABC News*. ABC News Network (March 19, 2016). http://abcnews.go.com/US/worldwide-hacker-group-anonymous/story?id=37761302.
[114] "Application Log," *Techopedia*, Techopedia Inc. (n.d.). https://www.techopedia.com/definition/1819/application-log.
[115] Tal Yellin, Dominic Aratari, and Jose Pagliery, "What Is Bitcoin?" CNNMoney. Cable News Network (n.d.). http://money.cnn.com/infographic/technology/what-is-bitcoin/.
[116] Intelligence and National Security Alliance, "Operational Levels of Cyber Intelligence," White Paper (September 2013). https://www.insaonline.org/CMDownload.aspx?ContentKey=cfdfcf7c-02b4-4507-a054-2606d684ffb0&ContentItemKey=bc0f998f-85f7-4db6-9288-903f748e1de9.
[117] NASCIO, *Cyber Disruption Response Planning Guide (*April 2016) p. 12. Retrieved on March 6, 2017 from http://www.nascio.org/Publications/ArtMID/485/ArticleID/358/.
[118] Merriam-Webster's Learner's Dictionary, "Cyberspace," *Merriam-Webster*. Merriam-Webster (n.d). http://www.merriam-webster.com/dictionary/cyberspace.
[119]"What Is a Botnet Attack? - Definition," Kaspersky Lab (N.p., n.d.). https://usa.kaspersky.com/internet-security-center/threats/botnet-attacks#.V-VS-_krKUk.
[120] "Bots and Botnets—A Growing Threat," *Norton*, Norton by Symantec (n.d.). https://us.norton.com/botnet/.

Business email compromise (BEC)—BEC is a scam in which criminal actors gain access to a legitimate business email account through social engineering or computer intrusion techniques. Cyber criminals commonly purport to be persons in high positions at a company and direct employees to send funds via wire transfer or check, or they ask for sensitive information such as employees' W-2 tax forms. BEC scams tend to be sophisticated and were responsible for a reported $1.2 billion in losses from October 2013 to August 2015.[121]

The Deep Web and the Dark Web—The Deep Web is a part of the World Wide Web whose contents are hidden and therefore not indexed by search engines. The vast majority of content on the Internet is hidden, including web mail, online banking, and most businesses' internal Intranets.

The Dark Web—The Dark web, by contrast, constitutes a smaller portion of the Deep Web that requires specific software or authorization to access networks. These networks are usually accessed through peer-to-peer connections or encrypted privacy networks like Tor or I2P. The Dark Web is the preferred tool for cyber criminals to conduct crime, including locating botnets, setting up commercial darknet markets (whereby criminals can sell or purchase items like drugs or guns), distributing child pornography, and planning terrorism.[122]

Denial of Service (DoS)—DoS is cyber crime in which a criminal actor attempts to make a machine or network unavailable to its intended users. These interruptions of service can be temporary or indefinite.[123]

- **Distributed denial of service (DDoS)**—DDoS is a particular type of DoS where a multitude of compromised systems all attack one target. This way, cyber criminals will flood a network with information to interrupt service, akin to a large group of people all trying to push through a door.
- **Telephony denial of service (TDoS)**—TDoS is another type of DoS where a high volume of calls, often originating from the Internet, flood a telephone or communications system to tie it up from receiving legitimate calls.[124]

Digital footprint—A digital footprint is the record of a user's activities in cyberspace. This record can be collected automatically as a user navigates the Internet (known as a passive digital footprint), or it can be left manually by users entering information into websites (known as an active digital footprint).[125]

---

[121] United States Federal Bureau of Investigation, Internet Crime Complaint Center (IC3), *Public Service Announcement: Business Email Compromise* (August 27, 2015) (N.p.). Alert number I-082715a-PSA. https://www.ic3.gov/media/2015/150827-1.aspx.

[122] Andy Greenberg, "Hacker Lexicon: What Is the Dark Web?" Wired, Conde Nast Digital (November 19, 2014). https://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/.

[123] Mindi McDowell, *Security Tip (ST04-015) Understanding Denial-of-Service Attacks*, United States Department of Homeland Security, United States Computer Emergency Readiness Team (US-CERT) (November 4, 2009) (N.p.). https://www.us-cert.gov/ncas/tips/ST04-015.

[124] Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," Wired, Conde Nast Digital (March 3, 2016). https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

[125] Eric Sheninger, "Your Digital Footprint Matters," *The Huffington Post*, TheHuffingtonPost.com (January 8, 2016). http://www.huffingtonpost.com/eric-sheninger/your-digital-footprint-ma_b_8930874.html.

Doxing—Doxing is a cyber crime in which criminal actors search for and publish private, sensitive, or identifying information about a victim on the Internet, often with malicious intent.[126]

Encryption—Encryption is the process of converting messages or information into encoded data so that it can only be accessed and read by authorized users.[127]

Firewall—A firewall is security software or hardware serving as the primary defense against unauthorized access to a computer network.[128]

Hacking—Hacking is the use of a computer to gain unauthorized access to data in a system.[129]

Hacktivism—A combination of "hacking" and "activism," hacktivism is the act of hacking into a computer system for politically or socially motivated purposes. For example, Anonymous posted personally identifiable information of Westboro Baptist Church (WBC) members online in 2012. The hacking group claimed the attack was in response to WBC's planned protest of funerals for victims of the Sandy Hook Elementary School shooting.[130]

Hard drive—A hard drive, also known as a "hard disk drive" (HDD), is a computer component used to store data such as files, documents, and media.[131]

Internet Protocol (IP) address—IP addresses are the numerical labels that serve as unique identifiers for every device connecting to a network that uses the Internet Protocol for communication. Network infrastructure may be assigned permanent (static) IP addresses, but most end-user devices are randomly assigned "dynamic" IP addresses upon connecting to a network.[132]

Internet Service Provider (ISP)—ISPs are organizations that provide services for accessing the Internet like Internet transit, domain name registration, web hosting, or Internet access.[133]

The Internet of Things (IoT)—IoT is the network of devices and physical objects that have embedded technology (e.g., sensors, software) that allows them to connect to the Internet. Examples of devices in

---

[126] Megan Garber, "Doxing: An Etymology," *The Atlantic*, Atlantic Media Company (March 6, 2014). http://www.theatlantic.com/technology/archive/2014/03/doxing-an-etymology/284283/.
[127] The Computer Language Company Inc., "Encryption," *PCMag Encyclopedia*, Ziff Davis, LLC. PCMag Digital Group (n.d.). http://www.pcmag.com/encyclopedia/term/42594/encryption.
[128] "Firewall: What It Is and How It Works," *Safety & Security Center*, Microsoft (n.d.). https://www.microsoft.com/en-us/safety/pc-security/firewalls-whatis.aspx.
[129] Vijay Prabhu, "Top Web Hacking Techniques of 2015," *TechWorm* (April 27, 2016) (N. p.). http://www.techworm.net/2016/04/top-web-hacking-techniques-2015.html.
[130] Eric Roberts, Ph.D., "What Is Hacktivism?" *Projects*, Stanford University (n.d.). https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/Hacktivism/what.html.
[131] The Computer Language Company Inc., "Hard Drive," *PCMag Encyclopedia*, Ziff Davis, LLC, PCMag Digital Group (n.d.). http://www.pcmag.com/encyclopedia/term/44088/hard-drive.
[132] The Computer Language Company Inc., "IP Address," *PCMag Encyclopedia*, Ziff Davis, LLC, PCMag Digital Group (n.d.). http://www.pcmag.com/encyclopedia/term/45349/ip-address.
[133] The Computer Language Company Inc., "ISP," *PCMag Encyclopedia*, Ziff Davis, LLC, PCMag Digital Group (n.d.). http://www.pcmag.com/encyclopedia/term/45481/isp.

the Internet of Things include smart phones, wearable technology like Fitbits, and modern automobiles and refrigerators.[134]

The Invisible Internet Project (I2P)—I2P is a project dedicated to creating an anonymous and encrypted network for cyber communication.[135]

Malware—Malicious software designed to inflict damage on a computer or its files. This software is often disseminated through email attachments and USB drives.[136] Common types of malware include:

- **Adware**—Adware is free application software containing advertisements. While adware may come in the form of legitimate software and not appear to be malicious, it often contains spyware capable of collecting users' data.[137]
- **Ransomware**—Ransomware is a type of malware that locks a computer system or its files, allowing attackers to demand a ransom from the user in exchange for restoring the system. Crypto-ransomware is a type of ransomware that locks a computer system or file through the process of encryption.[138]
- **Spyware**—Malware that secretly monitors users and is capable of stealing sensitive information. Spyware is often proliferated via free online software and emailed links.[139]
- **Trojan Horse**—Malware that appears to be a benign program but activates harm when opened.[140]
- **Virus**—Malware that spreads through a computer without the user's knowledge, causing system failures and file destruction.[141]
- **Worms**—Malware that replicates itself as it moves through a network, constantly seeking vulnerabilities in individual computers.[142]

---

[134] Nicole Kobie, "What Is the Internet of Things?" *The Guardian*, Guardian News and Media (May 6, 2015). https://www.theguardian.com/technology/2015/may/06/what-is-the-internet-of-things-google.
[135] Kate Knibbs, "I2P: The Super-Anonymous Network That Silk Road Calls Home," *Gizmodo*, Gizmodo Media Group (January 23, 2015). http://gizmodo.com/i2p-the-super-anonymous-network-that-silk-road-calls-h-1680940282.
[136] The Computer Language Company Inc., "Malware," *PCMag Encyclopedia*, Ziff Davis, LLC, PCMag Digital Group (n.d.). http://www.pcmag.com/encyclopedia/term/46552/malware.
[137] The Computer Language Company Inc., "Adware," *PCMag Encyclopedia*, Ziff Davis, LLC, PCMag Digital Group (n.d.). http://www.pcmag.com/encyclopedia/term/37577/adware.
[138] The Computer Language Company Inc., "Ransomware," *PCMag Encyclopedia*, Ziff Davis, LLC, PCMag Digital Group (n.d.). http://www.pcmag.com/encyclopedia/term/55712/ransomware.
[139] The Computer Language Company Inc., "Spyware," *PCMag Encyclopedia*, Ziff Davis, LLC, PCMag Digital Group (n.d.). http://www.pcmag.com/encyclopedia/term/51898/spyware.
[140] The Computer Language Company Inc., "Trojan," *PCMag Encyclopedia*, Ziff Davis, LLC, PCMag Digital Group, (n.d.). http://www.pcmag.com/encyclopedia/term/53178/trojan.
[141] The Computer Language Company Inc., "Virus," *PCMag Encyclopedia*, Ziff Davis, LLC, PCMag Digital Group, (n.d.). http://www.pcmag.com/encyclopedia/term/53963/virus.
[142] The Computer Language Company Inc., "Worm," *PCMag Encyclopedia*, Ziff Davis, LLC, PCMag Digital Group (n.d.). http://www.pcmag.com/encyclopedia/term/54874/worm.

Network—A network is a group of two or more devices that can communicate with one another over wired and/or wireless connections. Networks are typically comprised of many different computer systems.[143]

Network Intrusion—The malicious penetration of a network by an unauthorized user.[144]

Network Traffic Analysis—Network traffic analysis is the process of gathering and analyzing network information in order to review and enhance security and operational management, or conduct a cyber crime investigation. Hackers can also use network traffic analysis to perform a cyber attack.[145]

Packet Capture—Packet capture is the process of intercepting data travelling over a computer network. Packet capture can be used by system administrators or digital forensic specialists to diagnose network problems and build investigations, but it can also be performed by malicious actors seeking to steal information.[146]

Personally identifiable information (PII)—PII is identifying data unique to an individual that is stored electronically. Such information could include name, age, and contact information.[147]

Phishing—Phishing refers to fraudulent acquisition of personal information such as bank account information, account logins, and other sensitive data. Cyber criminals use phishing schemes to lure unsuspecting users into providing such information via email or web forms. These attacks are often highly sophisticated and appear to be legitimate.[148]

Reimaging—Reimaging is the process of restoring a computer's hard drive to an earlier copy of its files and settings.[149]

Silk Road—The Silk Road was a dark web marketplace used for black market transactions. The site was shut down by the FBI in 2013.[150]

---

[143] Florida Center for Instructional Technology, "Chapter 1: What Is a Network?" *An Educator's Guide to School Networks*, University of South Florida (n.d.). http://fcit.usf.edu/network/chap1/chap1.htm.
[144] Leonid Portnoy, Eleazar Eskin, and Sal Stolfo, *Intrusion Detection with Unlabeled Data Using Clustering*, Department of Computer Science, Columbia University (September 4, 2011). http://ids.cs.columbia.edu/sites/default/files/cluster-ccsdmsa01.pdf.
[145] Stephen Northcutt, Security Laboratory: Methods of Attack Series, SANS Technology Institute. http://www.sans.edu/research/security-laboratory/article/traffic-analysis.
[146] Darragh Delaney, "Packet Capture Made Simple," *ComputerWorld*, IDG (April 18, 2012). http://www.computerworld.com/article/2472879/networking/packet-capture-made-simple.html.
[147] "Protecting PII - Privacy Act," *Rules and Policies*, U.S. General Services Administration (November 18, 2015). http://www.gsa.gov/portal/content/104256.
[148] The Computer Language Company Inc., "Phishing," *PCMag Encyclopedia*, Ziff Davis, LLC, PCMag Digital Group (n.d.). http://www.pcmag.com/encyclopedia/term/49176/phishing.
[149] The Computer Language Company Inc., "Re-Imaging," *PCMag Encyclopedia*, Ziff Davis, LLC, PCMag Digital Group (n.d.). http://www.pcmag.com/encyclopedia/term/61431/re-imaging.
[150] Donna Leinwand Leger, "How FBI brought down cyber-underworld site Silk Road," *USA Today*, Gannett (May 15, 2014). http://www.usatoday.com/story/news/nation/2013/10/21/fbi-cracks-silk-road/2984921/.

Skimming—Skimming is an electronic method of stealing credit and banking card information when a user makes a transaction. Skimming can take place during a legitimate business transaction at an ATM or by using a handheld radio-frequency identification (RFID) reader to steal information from cards. [151]

Skype—Skype is a software application used for peer-to-peer video, audio, and messaging communication over the Internet, also known as Voice over Internet Protocol (VoIP). Most of Skype's services are free and available around the world.[152]

Software—There are two main types of software: system software and application software. System software is the operating system upon which a computer runs such as Microsoft Windows or Apple OS X.[153] Application software refers to a program loaded on to a computer to perform various functions such as Microsoft Word or Adobe Photoshop.[154]

Spoofing—Spoofing is the malicious practice of disguising oneself as a known source, such as a bank website or online shopping site, in order to fool an unsuspecting user for fraudulent gain.[155]

Swatting—Swatting is the false reporting of a crime to a law enforcement agency for the purpose of maliciously dispatching SWAT resources to an unsuspecting address. Attackers use a variety of techniques to perform this crime, including caller ID spoofing, and have been known to target celebrities and legislators. Many jurisdictions have enacted legislation regarding the practice.[156] [157]

The Onion Router (Tor)—Tor is a software application that enables users to conceal their identity and Internet activity from network traffic analysis. The software stacks layers of encryption on information

---

[151] Will Oremus, "The Skimming Scam," *Slate Magazine*, The Slate Group (August 25, 2015). http://www.slate.com/articles/life/travel_explainer/2015/08/credit_cards_passports_and_rfid_fraud_are_special_blocking_wallets_necessary.html.

[152] The Computer Language Company Inc., "Skype," *PCMag Encyclopedia*, Ziff Davis, LLC, PCMag Digital Group (n.d.). http://www.pcmag.com/encyclopedia/term/51443/skype.

[153] The Computer Language Company Inc., "System Software," *PCMag Encyclopedia*, Ziff Davis, LLC, PCMag Digital Group (n.d.). http://www.pcmag.com/encyclopedia/term/52419/system-software.

[154] The Computer Language Company Inc., "Application Software," *PCMag Encyclopedia*, Ziff Davis, LLC, PCMag Digital Group (n.d.). http://www.pcmag.com/encyclopedia/term/37931/application-software.

[155] The Computer Language Company Inc., "Spoofing," *PCMag Encyclopedia*, Ziff Davis, LLC, PCMag Digital Group (n.d.). http://www.pcmag.com/encyclopedia/term/51876/spoofing.

[156] Adrianne Jeffries, "Meet 'swatting,' the Dangerous Prank That Could Get Someone Killed," *The Verge*, Vox Media (April 23, 2013). http://www.theverge.com/2013/4/23/4253014/swatting-911-prank-wont-stop-hackers-celebrities.

[157] Jeff Stone, "What Is Swatting? Celebrities, Gamers And Now A Congresswoman Have All Been Targeted," *International Business Times*, IBT Media Inc. (February 2, 2016). http://www.ibtimes.com/what-swatting-celebrities-gamers-now-congresswoman-have-all-been-targeted-2289880.

similar to an onion. [158] The program was originally developed to increase military and government communications but is now available to the public.[159]

Victim-Centered Approach—A "victim-centered" approach is often discussed in the context of sex crimes, human trafficking, and other offenses involving special victims. For example, in the context of human trafficking, DHS defines a victim-centered approach as one that places equal emphasis on identification and stabilization of victims, with particular focus on ensuring that police do not retraumatize them.[160] Applying this concept to cyber investigations, police are recognizing the need to identify victims of cyber crime, help ensure their financial wellbeing, bolster their cyber security, and minimize any potential negative impact the investigation may have on victims.

Virtual Private Servers (VPS)—VPS is server space available for lease from an Internet host that can be used for both legitimate and malicious activity. Servers are computers dedicated to managing a network.

Voice over Internet Protocol (VoIP)—VoIP is technology that transmits communications data (voice calls, photos, and multimedia) between users using Internet Protocol (IP). VoIP is an accessible and low-cost communications method but lacks the security features offered by private networks. VoIP technology like Skype connects users around the world.[161]

[158] Raj Sabhlok, "Taking Stock Of Tor: Top 5 Tips For Using The Onion Router," *Forbes Magazine*, Forbes Media LLC (October 18, 2013). http://www.forbes.com/sites/rajsabhlok/2013/10/18/taking-stock-of-tor-top-5-tips-for-using-the-onion-router/#29f25bb1430e.
[159] Charles Graeber, "The Man Who Lit The Dark Web," *Popular Science*, Bonnier Corporation (August 30, 2016). http://www.popsci.com/man-who-lit-dark-web.
[160] https://www.dhs.gov/blue-campaign/victim-centered-approach.
[161] "Voice Over Internet Protocol (VoIP)," *Disability Rights Office*, Federal Communications Commission (n.d.). https://www.fcc.gov/general/voice-over-internet-protocol-voip.

Appendix: The State of Utah's Cyber Incident Response Plan

STATE OF UTAH

EMERGENCY OPERATIONS PLAN

ESF 2 Appendix

Cyber Incident Response

Primary Agency:	Department of Technology Services
Support Agencies:	Department of Public Safety
	State Intelligence Analysis Center
	Division of Emergency Management
	State Bureau of Investigation
	Utah National Guard
Other:	Department of Defense
	Department of Homeland Security
	Department of Justice
	Federal Emergency Management Agency
	Federal Bureau of Investigation
	Multi-State Information Sharing & Analysis Center
	University of Utah
	US Computer Emergency Response Team
	Private Sector

I. INTRODUCTION

A. Purpose

The purpose of this plan is to accomplish a coordinated response and recovery to cyber incidents involving the information technology (IT) systems and assets of local, state, tribal, and private entities.

B. Scope

The scope of this plan includes incidents that may be of a purely cyber nature, or a combination of cyber and physical impacts. These include localized, statewide, or national cyber incidents impacting critical infrastructure processes or economic activities.

This plan will define the organization, responsibilities, operational concepts, and actions pertaining to the state's response to a cyber incident.

During certain response operations, this plan may be used in conjunction with the State of Utah Emergency Operations Plan, its annexes, and/or other planning documents as required.

This plan is also intended to develop broad concepts for Utah's interface with three principal Federal Agencies. They are:

1. Department of Homeland Security (DHS). To include, but limited to:
    a) Office of Cybersecurity and Communications, which includes:
        (1) National Communications System (NCS)
        (2) National Cybersecurity Division (NCSD)
        (3) Office of Emergency Communications
    b) NCS's National Coordinating Center (NCC) for communications
    c) NCSD's United States Computer Emergency Readiness Team (U.S. CERT).
2. Department of Defense (DoD):
    a) The DoD Cyber Crime Center (DC3)
    b) U.S. Strategic Command, and Cyber Command
3. Department of Justice (DOJ) / Federal Bureau of Investigation (FBI)

II. POLICIES AND AUTHORITIES

A. The Cyber Security Emergency Support Function's (ESF) foundational authority is Executive Order D 011 04, December 6, 2004, which designates the National Incident Management System (NIMS) as the basis for incident management. Due to the unique aspects of a cyber incident of statewide or national significance an effective Unified Command is required. This Cyber Security document is built on the premise that the following partners will work together to form a NIMS Unified Command to coordinate the actions necessary for rapid identification, information exchange, response, and remediation to mitigate the damage caused by a cyber event:

1. Department of Public Safety (DPS)
2. Department of Information Technology (DTS)
3. Division Emergency Management (DEM)
4. State Bureau of Investigation (SBI)
5. Statewide Information and Analysis Center (SIAC)
6. Technology resources from the private and public sectors
7. Affected State Agencies

B. This document describes the specialized application of the National Response Framework (NRF) to cyber-related incidents. These cyber incidents may result in activation of the State's Cybersecurity Incident Response Team (CIRT) and Emergency Support Functions (ESF) that are part of the State Emergency Response Team (SERT). When processes in multiple annexes are activated, the State DEM continues its responsibilities under this Appendix and also fulfills its responsibilities as described in other annexes to the EOP.

C. The assets available to the Department of Public Safety will be used to assist other local jurisdictions and private sector entities with their emergency efforts as they relate to cyber incident response activities. The priorities for allocation of these assets are directly related to steady state, minor (3), moderate (2), or major (1) impacts to the following:

1. General Public Safety – Life/Death Situation (Human, Animal, and Environment)
2. National Security

3. Infrastructure

4. Criminal Activity

III. SITUATION & ASSUMPTIONS

A. Situation

Large scale cyber incidents may overwhelm government and private sector resources by disrupting the Internet and/or taxing critical infrastructure information systems. Complications from disruption of this magnitude may threaten lives, property, the economy, and national security. Rapid identification, information exchange, investigation, coordinated response, and remediation often can mitigate the damage caused by this type of malicious cyber activity. A cyber incident may occur at any time of day with little or no warning and will not be bounded by geographical features and may lack an easily identifiable signature.

B. Assumptions

1. Each State entity recognizes their own applicable cyber threats and will take reasonable precautions to protect their systems

2. Each entity will develop and maintain its own cyber incident response plan (this information may be incorporated as part of their Continuity of Operations Plan [COOP]).

3. Entities will devote the entirety of their cyber incident response capabilities and resources when invoking the State's Cyber Incident Response Team (CIRT) resources

4. State agencies and entities will accomplish all necessary notifications required by regulatory agencies

5. No single private or government agency or private sector entity possesses the authority or expertise to act unilaterally in all situations.

6. Government and private sector organizations will work together collectively on cyber related issues to protect critical infrastructure and develop plans and processes for restoring those systems in the event of a failure or compromise.

7. The response to and recovery from a cyber-Incident must take into account numerous existing challenges. Resources must be appropriately channeled to resolve identified challenges. Identifiable challenges include:

a) Management of Multiple Cyber Incidents – The occurrence or threat of multiple cyber incidents may significantly hamper the ability of responders to adequately manage the cyber incident. Strategic planning and exercises should be conducted to assist in addressing this issue.

b) Availability and Security of Communications – A debilitating infrastructure attack could impede communication needed for coordinating response and recovery efforts. A secure, reliable communications system is needed to enable public and private sector entities to coordinate efforts in the event that routine communications channels are inoperable.

c) Availability of Expertise and Surge Capacity – State agencies must ensure that sufficient technical expertise is developed and maintained within the State Cyber Incident Response Team (CIRT) to address the wide range of ongoing cyber attacks and investigations. Sufficient technical expertise may require in-place contracts with private sector entities that specialize in cyber incident response. In addition, the ability to surge technical and analytical capabilities in response to cyber incidents that may occur over a prolonged period must be planned for, exercised, and maintained.

d) Staffing to support the CIRT is limited – Requesting resource support from other entities will be needed. The National Guard has resources capable and available to support efforts and may be used if and when appropriate.

e) Coordination with the Private Sector – Cyber is largely owned and operated by the private sector; therefore, the authority of government to exert control over activities in cyberspace is limited.

IV. CONCEPT OF OPERATIONS

A. This section describes conceptually how the cyber response is implemented. Response is implemented using a formal cyber incident response process, including the following action steps:

1. Alert
2. Triage
3. Response

4. Recovery

5. Maintenance

B. Cyber Incident Source Authentication: It is critical that there is a mechanism to identify the authenticity of a reported cyber incident prior to committing CIRT resources. The Discovery Questionnaire is designed to assist with this issue. Two other sources can be used to assist with determining the authenticity of cyber incidents:

1. Authoritative (credible source) reports of the successful targeting of Utah's information infrastructure for exploitation, disruption, or destruction. This infrastructure includes the Internet, telecommunications networks, computer systems, and Industrial Control Systems (ICS) in critical industries.

2. Authoritative (credible source) reports of a cyber incident, either intentional or unintentional, that threatens Utah's economic prosperity through a loss of integrity of the communications and information infrastructure.

C. Response Activation:

1. DTS: Cyber security incidents will be handled internally for all supported state agencies that fall within DTS's purview. DTS will notify the State CIRT to include the DEM/SDO when a cyber incident reaches a severity level 4 or 5 as described in the DTS Cyber Incident Response Plan. The CISO will contact the DEM/SDO and CIRT Manager for team activation or another appropriate action.

2. Non-DTS Supported State Agencies and County/City Governments: IT managers from the applicable entities may contact the DEM/SDO for State CIRT team activation consideration at any time during the incident.

3. Private Sector: A private sector business or entity may contact the DEM/SDO for State CIRT team activation or another appropriate action based on existing or forecasted impacts to the surrounding community.

D. Notifications based on impacted entities:

1. DTS: When an incident requiring the State CIRT team activation occurs, a formal incident declaration will be made by the DTS CISO. Notification to State and local government political leaders and officers will be made by the DTS CIO and/or the State Agency Executive Director.

2. Non-DTS Supported State Agencies and County/City Governments: The State CIRT will make notification of potential cascading impacts to other State agencies and County/City government political leaders and officers.

3. Private Sector: The State CIRT will make notification of potential cascading impacts to other State agencies and County/City government political leaders/officers and other private sector entities.

E. Regulatory and Media Communication:

1. DTS: Mandatory reporting actions will be implemented in accordance with the DTS Cyber Incident Response Plan. Additional reporting to other agencies will be made through a collaborative effort between the CIO and the State CIRT. Notification to print and/or broadcast media will be made by the agency PIO or the DTS PIO based upon the affected agency's Executive Director's approval.

2. Non-DTS Supported State Agencies and County/City Governments: Mandatory reporting actions will be conducted as required by regulatory and State statutes. Additional reporting to other agencies will be at the discretion of the CIRT. Notification to print and/or broadcast media will be made by the agency PIO or the DEM PIO based upon the affected agency's Executive Director's approval.

3. Private Sector: Mandatory reporting actions will be conducted as required by regulatory and State statutes. Additional reporting to other agencies will be at the discretion of the CIRT. Notification to print and/or broadcast media will be made by the private sector entity and/or in collaboration with the DEM PIO based upon the effects of the cyber incident.

F. Alert Levels

1. Listed below are alert level protocols as established by the DEM, the CIRT, and Multi-State Information Sharing & Analysis Center (MS-ISAC). The alert level protocol alignment is displayed to understand when equivalent thresholds are reached and additional action may be required. Alerts consists of five levels:

Alert Level Equivalents		
DEM	CIRT	MS-ISAC
Daily Operations	Steady State	Green or Low
Level 3: Monitoring	Level 3: Minor (Monitoring)	Blue or Guarded
Level 2: Partial Activation	Level 2: Moderate (Partial Activation)	Yellow or Elevated
Level 1: Full Activation	Level 1: Major (Full Activation)	Orange or High
Continued Level 1	Continued Level 1	Red or Severe

2. Cyber Alert or Activation Levels 3, 2, and 1 consist of five identically named phases with actions that are appropriate for each increased level of incident severity. The cyclical phases are a continuous, monitoring, and improvement process. The phases are:

    a) Alert

    b) Triage

    c) Response

    d) Recovery

    e) Maintenance

G. Resources and Potential Sources of Incident Notification:

1. The MS-ISAC. The MS-ISAC is a voluntary and collaborative organization comprising all 50 States and the District of Columbia focused on raising the cyber security readiness and response in each State. The MS-ISAC will provide the following benefits to members:

a) Direct access to cybersecurity threat information from the State;

b) Access to security awareness materials, including computer - based training modules;

c) Access to security policy templates;

d) Access to security - related solutions at enterprise price points negotiated by the State; and,

e) Periodic meetings, teleconferences and webcasts to promote peer networking and information sharing.

2. The CIRT may deem it necessary to notify Federal or third-party support mechanisms to assist with the cyber incident. If so, facts will be provided to agencies that will develop National Requests For Information (RFIs) concerning response and recovery and immediately notify the U.S. Department of Homeland Security / National Protection and Plans Directorate / National Communications System (DHS / NPPD / NCS). Notification is made through established communications channels that exist between the Federal Government, nongovernmental entities, and the public. Such channels of communications include:

   a) National Cyber Alert System: This system provides an infrastructure, managed by US-CERT, for relaying timely and actionable computer security update and warning information to all users.

   b) Homeland Security Information Network (HSIN) Joint Regional Information Exchange System: This communications network provides States and major urban areas real-time interactive connectivity with the National Operations Center (NOC) through secure system carrying information on a Sensitive-but-Unclassified (SBU) level to all users.

   c) NOC: This is the primary national-level hub for domestic incident management communications and operations.

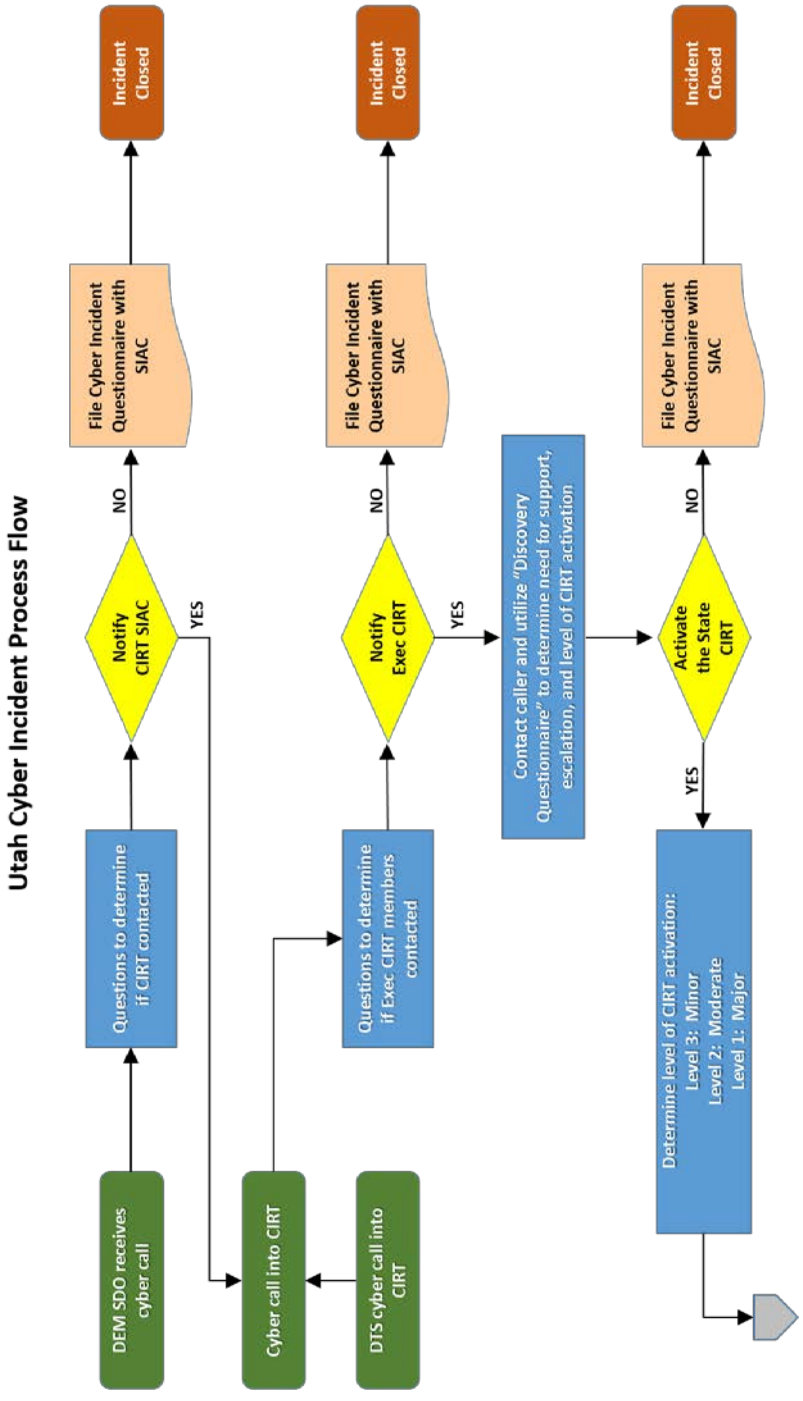
   d) Cyber Warning Information Network: This network provides out-of-band (i.e., not dependent on Internet or PSTN) connectivity to government and industry participants. The network is engineered to provide a reliable and survivable network capability.

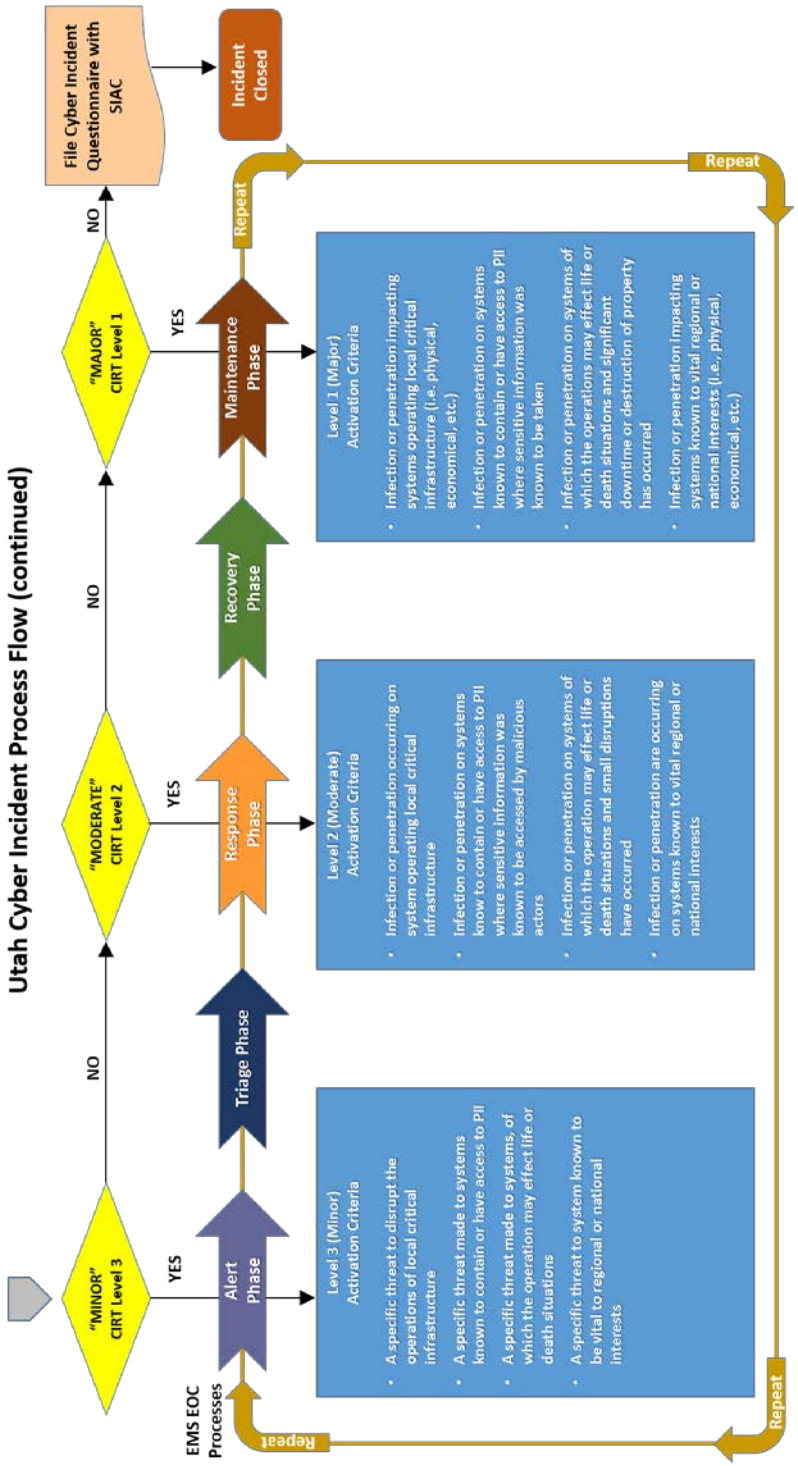
e) HSIN /US-CERT Portal: This is a secure collaboration tool for private and public sectors to actively converse about cyber security vulnerabilities, exploits, and incidents in a trusted environment among and between members.

f) Cyber Intelligence Network (CIN): The HSIN Cyber Sub-Committee, a collection of State Fusion Center Cyber Intelligence Analysts and SMEs.

g) US-CERT Public Web Site: This Web site provides the primary means for US-CERT to convey information to the public at large. The site includes relevant and current information on cyber security issues, current cyber activity, and vulnerability resources.

Actions Notification Process for CIRT Activation





See detailed instructions for the above notification tree in the Standard Operating Guidelines.

V. ROLES AND RESPONSIBILITIES

Primary Agency and Responsibilities for ESF #5

Primary Agency	Responsibilities
General: All agencies/organizations assigned to this plan	● Designating and training representatives for their agency to serve as primary points of contact (POC) to the State CIRT in the event of a cyber incident, and ensuring that appropriate action guides and Standard Operating Guidelines (SOGs) are developed and maintained. ● Identifying staffing requirements and maintaining current notification procedures to ensure appropriately trained agency personnel are available for extended emergency duty in the State Emergency Operations Center (EOC) if necessary. ● Developing and maintaining procedures to ensure that a current inventory of agency resources and contact lists are available as part of their COOP plans. ● Developing and maintaining procedures to identify, locate, commit, and deploy any agency support resources if requested by the CIRT as part of their COOP/DR Plan. ● Providing personnel, equipment, and other assistance to support emergency response and recovery operations within the agency's capabilities. ● Providing situational and operational situation reports in accordance with existing procedures and as requested by the primary agency. ● Should the resources of the Department of Public Safety (DPS) be overwhelmed and/or if the cyber incidents are widespread enough that a coordinated Federal response is invoked under the Federal National Cyber Incident Response Plan (NCIRP), the State's CIRT Manager will notify the applicable Federal Agency to request the necessary resources in accordance with the NRF and specific provisions of the NCIRP.

	● All support function members will be aware of their organization's capabilities for providing assistance and support. Support agencies will provide assistance in the form of personnel, equipment, and/or technical assistance as requested by the CIRT Manager.
DPS and DTS serve as primary agencies for State-level cyber threat analysis and/or incident response. As part of the State CIRT, they are responsible for State-level coordination of assets and services and will accomplish the following	● Identifying and coordinating support function staffing requirements appropriate to the emergency situation to include coordination of agencies' CIRT-trained resources as available. If a cyber-threat and/or incident has caused activation of the EOC to any extent, the Division of Emergency Management (DEM), in consultation with the SIAC and DTS, will be responsible for measures necessary to monitor and document the situation. ● Coordinating response to requests for assistance from the affected agencies, community-level government, and private sector entities through normal EOC procedures. In addition, the SIAC and DTS in conjunction with the EOC Operations Branch, coordinate the most feasible recommendations to designated direction and control authority for the mission assignment. ● Provide assistance to other agencies and local officials for data collection, documentation, and damage assessment for affected IT systems and in the disaster area(s) to include information on mitigation, recovery, and reconstitution options. ● Assist documentation preparation for departmental funding needs and develop priorities for state resource allocation. ● Assist in coordinating and monitoring state and non-state funded remediation efforts. ● Obtain and compile documentation/information necessary for effective and efficient strategy management by EOC and/or local EOC staff. ● Develop, maintain, and distribute any appropriate SOGs.

Support Agencies and Responsibilities for ESF #5

Support Agencies	Responsibilities
Division of Emergency Management (DEM)	● Coordinates with the Federal Emergency Management Agency (FEMA). ● Maintain the State Emergency Operations Center (EOC). ● Respond to the consequences of an incident through the guidelines of the State Emergency Operations Plan. ● Facilitates the coordination of recovery efforts. ● Manages the Joint Information Center (JIC) and serves as the lead for all messaging efforts to the public. ● Facilitates communications with other emergency entities involved in cyber incidents on a statewide basis. ● Coordination of training and education programs. ● When Cyber incidents result in the activation of the State CIRT, DEM in consultation with the State CIRT Manager, may activate components of the State Emergency Operations Center (EOC) to support the coordination of acquiring needed resources, coordinate public information support, and maintaining situational awareness. Examples of resources needed: ▪ DEM Public Information Support. A Joint Information Center or Joint Information System (JIC/JIS) will most likely be needed during large scale cyber incidents involving multiple agencies. The State EOC may facilitate and support these needs. Multiple PIOs from the affected agencies and/or jurisdictions may need to work together (in person or remotely) as a team to respond to media inquiries and produce unified messaging using a variety of methods. ▪ DEM may activate the State Emergency Response Team (SERT) in the Emergency Operations Center. If a cyber incident affects critical infrastructure or public safety, the SERT can manage the response for their respective ESF expertise.

	▪ DEM, in conjunction with the CIRT Manager, may produce situational awareness for state agencies and the Governor's Office. The SERT may produce daily situation reports, weekly briefings, or other documents to provide a common operating picture. ▪ The Policy Group in the EOC serves as decision maker for restoration priorities. When resources are overwhelmed and priorities must be determined, the Policy Group may work with the Governor's Cabinet to determine priorities.
State Emergency Operations Center (EOC)	● The EOC is responsible for Utah's interagency incident management and coordinating resources and information sharing during an incident. During a cyber emergency or disaster situation, the CIRT Manager will assign personnel to the EOC, as appropriate. ● The Department of Public Safety and the Department of Technologies Services are the primary agencies for State-level cyber threat and/or incident response. ● Through the EOC, the CIRT Manager and DEM will be responsible for leading the consequence management portion of the incident. ● The EOC will tailor supporting ESF personnel and materials from State Agencies specific to the cyber incident. The DTS and SIAC provide subject matter expertise related to the cyber threat, analysis, and recommendations to the EOC.
Department of Technologies Services (DTS)	● The mission of the Department of Technology Services (DTS) Cyber Security Incident Response Team (CSIRT) is to provide leadership in the development, delivery, and maintenance of an information security program by safeguarding the state's information assets against unauthorized use, disclosure, modification, damage, or loss to support Utah's mission to provide secure and sustainable services. ● DTS is directly aligned with the goals and objectives of the National Strategy to Secure Cyberspace. Working closely with federal, State, local, and private-sector partners, DTS actively gathers and analyzes information on cyber threats and vulnerabilities that present risk to

	select state agencies information systems or the critical information managed within. ● The Chief Information Security Officer is responsible for select state agencies' Information Security Program which include governance, risk, compliance, and risk management. ● The DTS Security Management is responsible for security and risk management for select state agencies. This group assists with development of State Information Security Policies and Security Standards. DTS addresses the onset of technical matters with select state agencies, and manages enterprise projects to meet security requirements. ● The DTS Compliance Program has oversight of applicable regulatory compliance of select state agencies to include compliance with federal and State laws, and regulations. ● The DTS Application Security Program is responsible for the creation of secure coding best practices to protect Utah's information systems and mission critical applications. ● For state agencies within the Executive Branch, DTS will be the decision maker, based upon information provided, for either taking the appropriate measures to halt the incursion / attack or to allow the incursion / attack to continue in an effort to gather forensics data in an effort to identify the perpetrator or gather evidence for prosecution. ● DTS maintains a cyber-response that may assist with national and/or state-level cyber security incidents. ● Any cyber insurance coverage maintained by DTS for the State Agencies may cover some of the resources needed during a cyber incident impacting select agencies, but it may take days to arrive.
SIAC / DEM	● Conduct threat information sharing both inside and outside the government, including best practices, investigative information, coordination of incident response, and incident mitigation. ● Assist in attributing the source of cyber-attacks through DEM resources and the national network of fusion centers.

	● Forensic analysis and support provided by DTS, SIAC, and SBI staff. ● Provide a top down conduit for information from DOJ and DHS to Utah State Government, and provide a bottom up and top down conduit to DOJ and DHS for information from the SIAC.
SIAC / DTS	● Conduit with the United States Computer Emergency Response Team (US-CERT) and the Multi-State Information Sharing and Analysis Center (MS-ISAC). ● Analyze cyber vulnerabilities, exploits, and attack methodologies. ● Provide technical assistance. ● Defend against an attack. ● Provide indications and warning of potential threats, incidents, and attacks. ● Support the coordination of acquiring needed resources and maintaining situational awareness. Examples of resources needed: ▪ Recruiting network admin expertise, private sector, such as Internet Service Providers ▪ Experts internal to associated State communications systems ▪ DHS cyber teams with forensic tools and resources ▪ Utah National Guard cyber team ▪ Vetted members of local cyber security working groups (i.e. UtahSAINT, Utah SEC, DC801, ISSA, ISACA, ISC2, etc.)
State Bureau of Investigation (SBI)	● SBI plays a major role in the cyber crime arena investigating criminal acts of cyber vulnerabilities, exploits, and attack methodologies. ● SBI's Cyber Crime Unit (CCU) investigates the criminal use of information technology. These crimes include but are not limited to computer and network intrusions, unauthorized access, data theft and Internet fraud. SBI Agents assigned to the CCU are also embedded with the FBI's Cyber Task Force. Agents hold a TS clearance with the FBI

	and are cross deputized so that they can investigate federal cases which can be brought to the U.S. Attorney's Office for prosecution. Agents work closely with the SIAC and DTS to assist with analyzing cyber attacks, identifying trends, and sharing intelligence. Agents also work with the Utah Crime Labs Forensics Services as well as with the FBI's Regional Computer Forensics Laboratory.
Various State Agency Support	● An IT security officer employed by each affected state agency may be designated to provide support to the CIRT as necessary.
Utah National Guard	● Included in the Utah Army National Guard (UTARNG) force structure is a specialized 10 pax Computer Network Defense Team (CND-T) consisting of Cyber professionals. The CND-T can be deployed in levels ranging from level 3 (minor) to level 1 (full), depending on the scope of the cyber incident. The specific capabilities, limitations, and support requirements of the CND-T are detailed in the CND-T Emergency Support Functions (ESF) Force Package. ● Within the law, and when ordered by the Governor of Utah, the Utah National Guard CND-T may provide the following cyber incident response capabilities: ▪ Cyber analysis including detailed examination of networks, systems, processes, and infrastructure. ▪ Threat and vulnerability assessment, including gaps in proper cyber posture. ▪ Information sharing, to include information regarding adversary tactics, techniques, and procedures. ▪ Digital forensics and investigation. ▪ Infrastructure and network monitoring support. ▪ Incident response, mitigation, and recovery. ▪ The CND-T can provide relevant cyber training and education, to include cyber exercises and best business practices.
FBI	● FBI Cyber Task Forces synchronize domestic cyber threat investigations in the local community through information sharing, incident response, and joint enforcement and intelligence actions.

	● FBI CyWATCH – Receives cyber threat and incident reporting, assesses it for action, and engages with the appropriate components within FBI Cyber Division, FBI field offices, other government agencies, and designated Federal Cyber Centers. ▪ May stand up a Cyber Incident Command Center (CICC) for enhanced coordination if the cyber incident is considered a significant or major incident defined by applicable Presidential Policy directive(s). ▪ May provide specialized and deployable on-scene forensic analysis to further attribution (would also depend on severity level). ● Intermountain West Regional Computer Forensics Lab (IWRCFL) – IWRCFL provides the highest quality digital forensics services and assistance to law enforcement agencies with jurisdiction in Utah, Idaho, and Montana. RCFL is a one-stop, full service forensics laboratory and training center devoted entirely to the examination of digital evidence in support of criminal investigation.
DHS	● The Department of Homeland Security (DHS): When cyber incidents occur, DHS provides assistance to potentially impacted entities, analyzes the potential impact across critical infrastructure, investigates those responsible in conjunction with law enforcement partners, and coordinates the national response to significant cyber incidents. https://www.dhs.gov/national-cybersecurity-and-communications-integration-center ● DHS's National Cybersecurity and Communications Integration Center (NCCIC) is a 24/7 cyber situational awareness, incident response, and management center that is a national nexus of cyber and communications integration for the federal government, intelligence community, and law enforcement. ● NCCIC's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT): Cybersecurity and infrastructure protection experts from ICS-CERT provide assistance to owners and operators of critical systems by responding to incidents and helping restore services, and by analyzing potentially broader cyber or physical impacts to critical infrastructure. ● NCCIC's National Cybersecurity Assessment and Technical Services (NCATS) offers cybersecurity scanning and testing services that

	identify vulnerabilities within stakeholder networks and provide risk analysis reports with actionable remediation recommendations. ● NCCIC's National Coordinating Center for Communications (NCC) leads and coordinates the initiation, restoration, and reconstitution of national security and emergency preparedness telecommunications services and/or facilities under all conditions. ● The National Infrastructure Coordinating Center (NICC), which is part of the DHS National Operations Center, is the dedicated 24/7 coordination and information sharing operations center that maintains situational awareness of the nation's critical infrastructure for the federal government. The NICC and the NCCIC share cyber and physical security information to enhance the efficiency and effectiveness of the U.S. government's work to secure critical infrastructure and make it more resilient. ● The Cyber Security Advisor (CSA) Program was created in recognition that a regional and national focused cyber security presence is essential to protect critical infrastructure. CSAs offer immediate and sustained assistance to prepare and protect SLTT and private entities. CSAs represent a front line approach to key cyber infrastructures throughout the U.S. and its territories. CSAs are regionally located based on the Federal Emergency Management Agency (FEMA) regions. Region VIII CSA is located in Denver. CSAs work closely with their Physical Security Specialist counterparts – the Protective Security Advisor (PSA) – who are located in every State.
Federal Government	● The Federal Government plays a significant role in managing intergovernmental (Federal, State, local, and tribal) and, where appropriate, public - private coordination in response to a cyber - incident. DHS / NPPD / NCSD, other elements of DHS, the Intelligence Community, FBI, DOD, and other Government agencies work closely together and individually to coordinate response during a cyber-incident or attack, identify those responsible, and otherwise respond appropriately. Responsibilities include: ▪ Providing indications and warning of potential threats, incidents, and attacks

	▪ Information - sharing both inside and outside the government, including best practices, investigative information, coordination of incident response, and incident mitigation ▪ Analyzing cyber vulnerabilities, exploits, and attack methodologies ▪ Providing technical assistance ▪ Conducting investigations, forensics analysis, and prosecution ▪ Attributing the source of cyber - attacks ▪ Defending against the attack ▪ Supporting recovery efforts
Roles and Responsibilities for Interagency Coordination	● A Unified Command arising from a cyber incident will be located in either DTS or the EOC. This recognizes that a cyber incident may not occur in isolation. Effective unified command is indispensable to response activities and requires a clear understanding of the roles and responsibilities of each participating organization. Success requires unity of effort, which respects the chain of command of each participating organization while harnessing seamless coordination across jurisdictions in support of common objectives. ● NIMS guides the State and Local government response, and NRF guides the Federal response. A critical aspect of a cyber incident is the ability to work effectively across organizational boundaries as primary responsibility for a cyber incident may pass between agencies. Establishment of liaison officers between agencies and the private sector is critical. Within this framework Utah has further identified initial cyber responses by identifying a Cyber Incident Response Team (CIRT) composed of various state agencies. The CIRT is comprised of the following members that are activated depending on the level of cyber incident impacts: ▪ SIAC ▪ DTS ▪ EOC

	▪ FBI ▪ Utah National Guard ▪ University of Utah Security Operations Center (SOC) ▪ Other entities based on their desire to participate and type of incident ● Support agencies are those entities with specific capabilities or resources that support the State Cyber Incident Response Team that include: ▪ Representative from impacted agency, or private sector ▪ Third-Party Vendors ▪ Parties activated as a result of the impacted entities insurance policy ▪ State Risk Management

VI. AUTHORITIES AND REFERENCES

Provided below are the major authority and reference documents related to the implementation of this emergency management plan for state response to cyber incidents:

A. State:

1. House Bills
2. State Emergency Operations Plan
3. State IT Strategic Plan
4. State Enterprise Security Plan
5. State Cyber Incident Management Plan
6. Department of Technology Services Cyber Security Incident Response Plan
7. Each State Agency's Continuity of Operations Plans and/or Cyber Security Incident
8. Response Plans

B. Federal:

1. The National Incident Management System (NIMS) is the framework that provides a consistent nationwide template to enable all government, private-sector, and nongovernmental organizations to work together during domestic incidents.

2. Homeland Security Act of 2002 provides the basis for Department of Homeland Security (DHS) responsibilities in the protection of the Nation's CI. The act assigns DHS the responsibility for developing a comprehensive national plan for securing CI and for recommending the measures necessary to protect the CI of the United States in coordination with State and local agencies and authorities, the private sector, and other entities.

3. Homeland Security Presidential Directive 7 provides a unifying framework for national approach for CI protection. This directive establishes the United States policy for enhancing protection of the Nation's CI and mandates a national plan to actuate that policy.

4. Defense Production Act provides the primary authority to ensure the timely availability of resources for national defense and civil emergency preparedness and response.

5. The Communications Act of 1934 provides the Federal Communications Commission (FCC) authority to regulate interstate and foreign commerce in communications by wire and radio, making available rapid and efficient nationwide and worldwide wireless and wireline communications services to United States residents. This act, among others, is vital to national defense and promotion of the safety of life and property. The FCC's interest in cyber security is rooted in this act.

6. Provided below are the major authority and reference documents related to the implementation of this cyber plan for the State of Utah's response to cyber incidents.

Jurisdiction	Legislation/Authorization References
Federal	• National Response Framework, Second Edition, May 2013 https://training.fema.gov/hiedu/highref/national%20response%20framework-second%20ed-may%202013-natresp.pdf • National Incident Management System (NIMS) https://www.fema.gov/national-incident-management-system • National Institute of Standards and Technology (NIST) Special Publication 800-61 Revision 2, Computer Security Incident Handling Guide http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
State	• DTS Cyber Response Plan • Utah Technology Governance Act H.B.109 (2005) https://le.utah.gov/~2005/bills/static/HB0109.html • Utah Code Title 63F (Utah Technology Governance Act) Chapter 1 – 101 http://le.utah.gov/xcode/Title63F/Chapter1/63F-1-S101.html • SBI/SIAC Cyber Crime Guidance • Commissioner Squires Directive to Create a Cyber Plan

VII. SUPPLEMENTAL DOCUMENTS

Standard Operating Guidelines, Checklists, Glossary and other supplemental documents are found in the EOC Binders for ESF #2. When Internet access is available, follow these links to the supporting information:

Standard Operating Guidelines

Support Document, Cyber Support within the State EOC

Glossary