June 2016

Issue Brief # 2016-01

Cybersecurity for State and Local Law Enforcement: A Policy Roadmap to Enhance Capabilities

Center for Cyber & Homeland Security
THE GEORGE WASHINGTON UNIVERSITY

National Consortium
NCAP
for Advanced Policing

CYBERSECURITY FOR STATE AND LOCAL LAW ENFORCEMENT: A POLICY ROADMAP TO ENHANCE CAPABILITIES

Introduction

In recent years, cybersecurity has become a significant strategic priority for governments and for the private sector. For senior government officials and company executives, achieving and maintaining cybersecurity and cyber-resilience is an ongoing and necessary operational imperative. Consistent with this broader trend, cybersecurity has also become a strategic area of concern and responsibility for state and local law enforcement agencies.

This issue brief is a companion to the *NCAP Cybersecurity Guide for State and Local Law Enforcement*, a comprehensive and practical guide on cybersecurity for state and local law enforcement that is being released in June 2016 by the National Consortium for Advanced Policing.[1] This issue brief instead focuses on how policy-makers at federal, state and local levels, both in the executive and legislative branches of government, can take steps to improve the cyber authorities and capabilities of state and local law enforcement.

The range of threats facing government entities and the private sector is dizzying. State actors and their security and intelligence services possess both the capability and intent to target and damage US interests. Non-state actors also have developed sophisticated cyber skills and provide their nefarious services to the highest bidder or to the entity whose ideology and objectives they admire and espouse. Proxy forces, along with the increasing convergence of terrorist and criminal groups in the cyber domain, make for a dangerous ecosystem.

Against this background, law enforcement agencies and officials at the state and local levels are assuredly not immune. Already we have seen cyber-attacks on local police departments, as well as fusion centers, and these are only the incidents that we actually know about. There may well be others underway but not yet discovered; and yet more that are in the planning stages. Granted, the nature of the damage caused to people, equipment, privacy, and so on, may vary widely. However, even at the lower end of the spectrum where there is no loss of life or physical harm done to any

[1] The *NCAP Cybersecurity Guide for State and Local Law Enforcement* is available on the websites of the GW Center for Cyber & Homeland Security (http://cchs.gwu.edu) and NCAP (http://www.advancedpolicing.com), or by e-mailing NCAP at info@advancedpolicing.com.

individual, there may be significant implications for state and local law enforcement authorities – including in the form of (always-scarce) resources that must be diverted to address and resolve such cyber events.

With all of these considerations in mind, it is important to ask whether we are doing all that we can, as a nation, to meet and defeat these challenges both as they exist today and as they are likely to develop in future. While there is no single silver bullet solution, there are many steps that can be taken by agencies and entities at all levels of government to enhance their cybersecurity capabilities, both with respect to protecting their own networks and information, and improving the overall cybersecurity of communities.

A. The Federal Dimension: Executive Branch

There are several things that federal entities can and should do to support cybersecurity efforts at the state and local levels. The first is improving working relationships between federal authorities and their state and local counterparts. Presently, they are not as strong or clear as they could be. The situation is compounded by the fact that the national cybersecurity mission is spread far and wide across the many and varied entities of the federal government (and beyond). Unless federal officials exercise substantial care in their outreach the state and local levels, the coordination will never truly come together and the potential for conflict will continue to exist.

In addition to improved coordination, lending resources in the form of cybersecurity experts can have a lasting impact on the resource-scarce environments that prevail at the state and local levels. For example, more liaison officers with wide-ranging expertise could be dispatched from the federal level to state and local agencies. This would expand the latter's cybersecurity operational capabilities, improve policies and encourage the greater dissemination and implementation of best practices nationwide. This approach must be in principle and practice one of genuine partnership. Since cyber challenges have no regard for borders or boundaries, our response must be equally seamless.

<u>Recommendations for the Federal Government</u>

1. The federal government needs a clearer strategy for its engagement with state and local law enforcement agencies on cybersecurity. In many parts of the country, these relationships are not as robust as they should be, due

to interagency rivalry at the federal level, unclear policies for coordination and de-confliction of investigative activities, and resource challenges.

2. The Department of Homeland Security and Department of Justice should increase state and local cybersecurity as a priority area for grants made by DHS under the Homeland Security Grant Program and by DOJ through the Office of Justice Programs.

3. The Department of Justice and Department of Homeland Security should carry out cybersecurity audits of federal-state or multi-state law enforcement information systems (e.g. RISS, Law Enforcement Online) that they currently fund, utilize or otherwise support. The Inspectors General of these two Departments may also want to carry out audits on such systems.

4. DHS should deploy additional staff from its Office of Cybersecurity and Communications to liaison with state and local agencies on cybersecurity operational and policy matters. Such liaison activities should be coordinated with the Office of Infrastructure Protection's Protective Security Advisors program and the DHS Office of Intelligence and Analysis' intelligence officers program.

5. These agencies should work with state and local governments to develop cybersecurity standards and best practices for state-wide law enforcement information systems.

6. The Department of Justice should initiate and lead a process to update 28 CFR Part 23, the federal regulation governing criminal intelligence systems that receive funding from the Department of Justice, to reflect and clarify state and local law enforcement agencies' roles with respect to cybersecurity threats and investigations, and ensure that agencies are appropriately handling and safeguarding personally identifiable information (PII) that is collected in investigations. This process should include a wide group of stakeholders, including state and local agencies and civil liberties groups. In tandem with this effort, the Department of Justice should provide policy recommendations for agencies that are governed – either in addition to 28 CFR Part 23 or instead of – by their agencies' own intelligence guidelines.

7. DHS and other federal agencies need to involve state and local partners in the process of implementing new policies and guidelines for cyber threat information sharing following the enactment of the Cybersecurity Act of 2015.[2]

8. The DHS S&T Directorate and the National Institute of Justice (NIJ) should fund applied research on state and local requirements for cybersecurity, and encourage partnerships between academia and state and local agencies on cybersecurity research projects.

B. The State and Local Dimensions: Executive Branch and Law Enforcement

Akin to the federal level, the primary responsibility of state and local governments and their law enforcement agencies is to place their own houses in order from a cybersecurity perspective. Currently, maturation levels in this regard differ substantially from locality to locality. While the granular details will differ by specific location, these various plans and structures should all reflect the importance of cybersecurity within the universe of competing governance priorities. Governors, mayors, and other officials must demonstrate leadership to address these challenges, and must designate and empower a specific high-level point of contact within their administrations to shepherd cybersecurity initiatives that foster vigilance and resilience.

Similar leadership efforts are required on the part of senior law enforcement officials who helm the nation's thousands of state and local law enforcement agencies. These leaders face budgetary and other constraints that may present even more acutely than at the federal level. Added to these agencies' panoply of urgent responsibilities, cybersecurity challenges stretch even thinner an already-taxed system. In such context, there is understandably little time or resources to train the workforce on basic cyber-hygiene practices, or to continually test their ongoing appreciation and implementation of cybersecurity considerations and necessities. While doing so will certainly entail time and effort, it is essentially an imperative rather than a choice given the interlinked nature of the cyber domain that we all operate in daily.

[2] The Cybersecurity Act of 2015 can be found at this link: http://www.intelligence.senate.gov/sites/default/files/legislation/Cybersecurity-Act-Of-2015.pdf

C. The Legislative Dimension: Congress and State Legislatures

On the legislative side at the federal level, Congress was until recently largely deadlocked in terms of achieving progress on critical cybersecurity matters. Building on recent momentum, there is an opportunity for Congress to act in ways that would increase the effectiveness of cybersecurity efforts nationwide. Specifically, Congress could identify and pursue avenues to heighten its support for state and local law enforcement agencies. These measures would include underwriting cybersecurity training and technical assistance, and by conducting oversight of federal cybersecurity activities that substantially benefit their state and local counterparts. The run-up period to the 2016 elections and their immediate aftermath offer important windows for Congress to specify its priorities and move forward on them.

On the legislative side at the state level, there is the ability to mandate and fund cybersecurity programs that deepen state and local capacities in critical areas like threat detection and attribution. To the extent that the areas targeted also dovetail with federal efforts—meaning complement but not simply duplicate—such initiatives could have exponential impact. State legislatures also are uniquely positioned to de-conflict and synergize the various cybersecurity-related strategies and strands of activity that state officials have already developed and begun to implement.

<u>Recommendations for the U.S. Congress and State Legislatures</u>

1. Congress should consider increasing funding to support cybersecurity training and technical assistance for state and local law enforcement agencies.

2. Congress should conduct oversight as to whether federal agencies are complying with the objectives of the unified message for Law Enforcement Cyber Incident Reporting, released in 2014.[3]

3. State legislatures should require that governors develop state-level strategies for cybersecurity, and should consider legislation (as needed) that clarifies the relationship among officials with responsibility for different aspects of cybersecurity policy and governance. State

[3] Available at https://www.fbi.gov/about-us/investigate/cyber/law-enforcement-cyber-incident-reporting

legislatures may also want to provide state CISOs with clearer statutory authority with respect to their roles and responsibilities.

4. State legislatures should mandate that their state governments develop insider threat programs, led by the state Attorney General and supported by the state CIO and state personnel/administration office.

5. State legislatures should fund the development of enhanced cyber forensic capabilities at the state level, in coordination with a federal effort to fund such capabilities.

Conclusion

Cybersecurity challenges continue to evolve in scope and sophistication. Since our adversaries are adaptive, our responses must also reflect such learning. Precisely because the ground is ever-shifting in the cyber domain, there must be mechanisms for recognizing and adjusting to new and prevailing realities, and for incorporating same into both curricula and culture/mindset. Regular communication—with an eye to action—between and among stakeholders in the national cybersecurity enterprise is critical. So too is building awareness and knowledge of cybersecurity matters at an earlier stage in the process than is now the case (*i.e.,* pre-workforce/educational) so that that foundation can later be leveraged in response to changes in the cyber ecosystem.

<u>Recommendations for all stakeholders</u>

1. Key federal, state and local stakeholders should regularly meet to discuss key policy issues, and revise the National Criminal Intelligence Sharing Plan and other strategies to reflect emerging cybersecurity requirements.

2. Cybersecurity courses should be required within all undergraduate criminal justice programs, and specialized masters' programs should be increased for cyber investigation and forensics.

The actions recommended above, if implemented, would lead to positive improvements to state and local law enforcement cybersecurity capabilities, and would ultimately enhance their role as critical partners to the federal government in addressing a broad range of cyber threats.