NATIONAL SHERIFFS' ASSOCIATION
CYBERSECURITY & CRIME WORK GROUP

THE RECOMMENDED PATH FORWARD ON CYBERSECURITY FOR SHERIFFS & THEIR PARTNERS

December, 2022

Sheriff David Goad (Ret.), Chair
Dennis Kelly, Esq., Vice Chair
Work Group Executive Committee

DISCLOSURE

This Report reflects the work of the National Sheriffs' Association ("NSA") Cybersecurity & Crime Work Group (the "Work Group") on behalf of its primary constituency, Sheriffs and their local law enforcement partners, including, especially, Municipal Police Departments and local prosecutors with whom Sheriffs work daily.

Inherently, the Work Group is composed of persons who are highly concerned about the effectiveness and efficiency of local law enforcement, many of whom are concerned about best practices being available to and used by law enforcement in dealing with the cyberthreat, and many of whom are directly involved with and knowledgeable of cybersecurity and cybercrime, including cybersecurity best practices and a broad range of cybersecurity solutions.

As a result of these overlapping relationships, it is common for persons involved with the Work Group to be directly involved with and/or have an interest in one or more cybersecurity best practices and/or solutions that are of interest to the Work Group.

It is acknowledged here that one or more contributors to this Report are affiliated with one or more suppliers of one or more of the cybersecurity approaches recommended as paths forward here. In an effort to be vendor neutral, this Report does not recommend any vendor for any of these approaches or solutions, and limits its discussion of possible vendors of services that Sheriffs and other members of its primary constituency may want to contact regarding the availability of services aimed at achieving the approaches recommended here.

It is anticipated that this Final Report of the Work Group will be presented to the NSA Homeland Security & Global Policing Committee ("Committee") at the NSA Mid-Winter Conference to be held in Washington, DC in February 2023. Since the Work Group is a creature of the Committee, this Report is subject to input by that Committee and/or by the NSA Board of Directors.

In the event of questions or comments about this document, please contact:
Sheriff David Goad (Ret), Past NSA President, 301-268-2901 or dgoad78@gmail.com

####

NATIONAL SHERIFFS' ASSOCIATION
CYBERSECURITY & CRIME WORK GROUP

THE RECOMMENDED PATH FORWARD ON CYBERSECURITY FOR SHERIFFS & THEIR PARTNERS

DECEMBER, 2022

BACKGROUND ON THE WORK GROUP AND THIS REPORT

This Report is part of the response to the charge put to Sheriff David Goad, Past NSA President, in 2017, that he form a work group to provide a recommended path forward for NSA, Sheriffs, and their Local Law Enforcement partners on Cybercrime Investigations for their constituencies and on Cybersecurity for their Offices and Agencies. In response to that charge, Sheriff Goad led the organization of the NSA Cybersecurity & Crime Work Group (the "Work Group"), and the some 60 monthly Work Group meetings since its organization in 2018.

The Path Forward on Cybercrime

In response to NSA's charge to recommend a path forward for Sheriffs and their Law Enforcement Partners on Cybercrime Investigations, the Work Group developed a two-pronged recommended path forward, consisting of development of a) **the National Cybercrime Investigators Program (NCIP),** a program aimed at providing Cybercrime Investigation Training and Certifications for Local Law Enforcement[1], and b) the **HANDBOOK FOR THE NCIP CYBER INVESTIGATIONS PROGRAM[2],** a handbook on how local law enforcement agencies might organize for their efforts to investigate cybercrimes, which was published in June 2021.

The Path Forward on Cybersecurity

This Report reflects the findings of the NSA Work Group on the Recommended path forward on Cybersecurity for the Nation's Sheriffs' Offices and their partners.

The Next Steps for the Work Group

In 2022, the Cyberthreat is still global in nature, and still has not diminished and reduced its potential impact on the Office of Sheriff, both in terms of Cybersecurity of Sheriffs' IT Systems and in terms of Cybercrimes committed against Sheriffs' Systems and against the communities that Sheriffs' have sworn to protect and serve.

Indeed, the cybersecurity of Sheriffs' IT Systems and the proliferation, globally, of Cybercrime which call for attention by Sheriffs and their law enforcement partners, clearly indicate the need for increased attention, not less, by law enforcement working

- The still anticipated massive deployment of Internet of Things devices and other Smart City sensors and technologies that will directly impact the work of Sheriffs and their law enforcement and public safety partners;

[1] See https://www.ncip.tech/.

[2] See **HANDBOOK FOR THE NCIP CYBER INVESTIGATIONS PROGRAM**, https://img1.wsimg.com/blobby/go/6754d4ea-d143-490a-a31b-1d2bf066d416/210614%20NCIP%20CYBER%20INVESTIGATIONS%20HANDBOOK%20Comp.pdf.

- The anticipated deployment of large numbers of Electric Vehicles and Electric Vehicle Charging Systems which will introduce many new vulnerabilities
- The anticipated reinvention of the Grid, and the electric generation and distribution system, including the introduction of many new types of electric generation, new patterns of electricity distribution, entirely new energy storage systems, and many new players who have not yet created a common culture of physical and cybersecurity
- The increasing use of cryptocurrencies in commission of crimes and the anticipated increasing use of cryptocurrencies and crypto assets in routine commercial life;
- The anticipated massive deployment Artificial Intelligence technologies and systems that will be a source of new tools for law enforcement and new cybersecurity threats and new cybercrimes;
- The inherent delay of developing and publishing best practices in these and other technology deployments that lead to technical and societal dysfunction and, from the perspective of customers and end-users, less than optimal service offerings and less than optimal deployments
- The seemingly ever-increasing role of State Actors in conducting cyber attacks
- The shrinking of the globe in everyday life of the average person, in terms of international travel, international commerce, and international family and other interpersonal relationships that lead to calls for service, public safety challenges
- The increasing possibility of global pandemics and global weather patterns that dramatically impact the work of Sheriffs and their local law enforcement partners; and
- Other developments we have not even come to understand yet.

Accordingly, the Work Group will continue its work in support of Cybersecurity and investigation of Cybercrimes, under the purview of the NSA Homeland Security & Global Policing Committee, by, among

- Continue working with the Uniform Law Commission on a Uniform State Cybercrime Law, http://uniformlaws.org/home, that is presented to the 50 State Legislatures for enactment.
- Continue working with the Paris Peace Forum on its Paris Call for Trust and Security in Cyberspace, https://pariscall.international/en/, aimed at increasing global cooperation and collaboration on cybersecurity and cybercrime investigations among civil society actors, worldwide.
- Continue working with NSA and the NSA Homeland Security & Global Policing Committee, especially regarding:
    - Obtaining local law enforcement access to no-cost training on cybercrime investigations
    - Obtaining funding to provide local law enforcement with cybercrime investigation information sharing and collaboration resources and investigative tools

  - Obtaining funding to provide local law enforcement training on managing the human factor within departments to avoid the risk of intentional internal threats affecting departmental operations, including the insider cyber threat
- Continue working toward increased collaboration and cooperation by and among Sheriffs and their domestic U.S. local law enforcement partners in fighting the cyberthreat;
- Putting new focus on Sheriffs' Global Policing needs by increased collaboration and information sharing with international partners

A CYBERSECURITY LESSON LEARNED FROM THE SHIPPING INDUSTRY

A Lesson from the Shipping Industry

Unlike the cybersecurity industry, the global shipping industry is a hoary commercial enterprise perhaps as old as civilization itself. Over the centuries, the shipping industry has learned—the hard way—the imperative of achieving safety at sea, and, in response, has implemented a highly developed operational culture and set of systems and practices built around safety on board ships at sea.

In April, 2022, the World Maritime University hosted a webinar to introduce a ground-breaking White Paper entitled "Towards a Safety Learning Culture for the Shipping Industry".[3] That White Paper, developed within the framework of the European Union-funded SAFEMODE project,[4] was built around a maritime-aviation partnership that enabled a first ever comparative analysis of safety protocols and practices of the the shipping and aviation industries. In essence, after having developed and practiced over hundreds of years a well-defined set of sea safety protocols and practices, a new maritime safety protocol—a Safety Learning Culture—was found to be needed after evaluating what previously had been practiced. This was the result of approaching the problem with a fresh perspective, and significantly re-working lessons previously learned in light of new findings.

Upon Looking at Cybersecurity from a Fresh Perspective, New Approaches are Recommended

In some ways, this Report reflects an effort by the Work Group to look at well-established cybersecurity practices and protocols with a fresh perspective. As such, the Work Group believes this exercise has been an important Cybersecurity learning experience, and urges that Sheriffs and their partners in local law enforcement—indeed, every agency within the Emergency Services Sector—carefully consider implementing these recommendations.

In this vein, this Report recommends that Sheriffs and their local law enforcement partners and, indeed, the entire Emergency Services Sector, carefully consider three new—or refreshed—approaches to cybersecurity going forward. Those approaches are discussed in three Parts below, as follows:

PART 1: TO MEANINGFULLY ADDRESS THE CYBERTHREAT, IT IS IMPERATIVE THAT CYBERSECURITY MANAGERS FIRST FOCUS/REFOCUS ON ADDRESSING THE CYBERSECURITY FUNDAMENTALS, AS ARTICULATED IN THE NIST CYBERSECURITY FRAMEWORK.

[3] **SAFEMODE, Towards a Safety Learning Culture for the Shipping Industry: A White Paper** (April, 2022), https://safety4sea.com/wp-content/uploads/2022/05/SAFEMODE-Safety-Learning-White-Paper-2022_05.pdf.

[4] **SAFETY4SEA, SAFEMODE project: Ten good practices for enhancing Safety Learning** (May 24, 2022), https://safety4sea.com/safemode-project-ten-good-practices-for-enhancing-safety-learning/.

THE RECOMMENDED PATH FORWARD ON CYBERSECURITY FOR SHERIFFS & THEIR PARTNERS

PART 2: TO MEANINGFULLY ADDRESS THE CYBERSECURITY INSIDER THREAT, CYBERSECURITY MANAGERS MUST LOOK BEYOND TECHNICAL THREAT VECTORS, AND ALSO CONSIDER NON-TECHNICAL HUMAN BEHAVIORAL THREAT VECTORS.

PART 3: TO MEANINGFULLY ADDRESS THE CYBERTHREAT, LOCAL LAW ENFORCEMENT CYBERSECURITY MANAGERS MUST LOOK BEYOND TRADITIONAL LOCAL LAW ENFORCEMENT ORGANIZATIONAL BOUNDARIES, AND FIND AND IMPLEMENT NEW CYBERSECURITY APPROACHES THAT WORK IN THE REAL WORLD.

THE RECOMMENDED PATH FORWARD ON CYBERSECURITY FOR SHERIFFS & THEIR PARTNERS

PART 1: TO MEANINGFULLY ADDRESS THE CYBERTHREAT, IT IS IMPERATIVE THAT CYBERSECURITY MANAGERS FIRST FOCUS/REFOCUS ON ADDRESSING THE CYBERSECURITY FUNDAMENTALS, AS ARTICULATED IN THE NIST CYBERSECURITY FRAMEWORK.

BACKGROUND: THE NIST CYBERSECURITY FRAMEWORK "CORE FUNCTIONS"

The National Institute of Standards and Technology ("NIST") Cybersecurity Framework is widely recognized to be the preeminent cybersecurity "best practices" document for any organization's cybersecurity plan and efforts. It is the starting point and foundation for the Work Group's recommendations. It provides five "Core Functions" that should be the cornerstone for any Cybersecurity effort for U.S. local law enforcement, as follows:

NIST Cybersecurity Framework Core Functions[5]
Identify – Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities. ...
Protect – Develop and implement appropriate safeguards to ensure delivery of critical services. ...
Detect – Develop and implement appropriate activities to identify the occurrence of a cybersecurity event. ...
Respond – Develop and implement appropriate activities to take action regarding a detected cybersecurity incident. ...
Recover – Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. ...

WORK GROUP INQUIRY AND INVESTIGATION

After diligent search and investigation conducted in 2018, the Work Group was unable to find any approach to cybersecurity that could be recommended as a path forward for local law enforcement. This was primarily because the Work Group found no solution that meaningfully addressed the first three of these NIST "Core Functions"—**"Identify", "Protect"** and **"Detect"** (the "Cyberdefense Core Functions"—and that was affordable as a real world path forward for U.S. local law enforcement agencies. Accordingly, the Work Group suspended its investigation into a "path forward" on Cybersecurity and turned its attention to "Cyber Crime".

FINDINGS

In 2021, the Work Group, having previously reported to NSA on its recommended path forward on "Cyber Crime", again turned its attention to a path forward on "Cybersecurity" and found that material progress had been made in that area. Specifically, the Work Group found that multiple realistic, affordable and mature solutions had become available to local law enforcement to meaningfully address the three Cyberdefense Core Functions, namely:

[5] **NIST Cybersecurity Framework Version 1.1**, pp.7-8 (April 16, 2018).

Cyberdefense Core Function	Delivery Vehicle
Identify	**Organizational Cyber Maturity Programs**
Protect	**Continuous Network Monitoring**
Detect	**Real-Time Vulnerability Assessment**

-The Identify Core Function. While all of these Cyberdefense Core Functions are equally vital, fulfilling the Identify Core Function by achieving "Cyber Maturity" is, ultimately, the most important because, until an organization achieves Cyber Maturity, it can never be, in any meaningful sense, "cybersecure". Moreover, the efforts required to achieve Cyber Maturity can be done totally internally, without any payment to anyone other than agency personnel. And, because these efforts involve organizational processes that can be led by an agency's C-Level Management and understood by anyone within law enforcement (as opposed to technical IT or "Cyber" processes), achieving Cyber Maturity is readily achievable, with effort, by every local law enforcement agency in the Nation. Accordingly, the Work Group highly recommends that NSA and every U.S. law enforcement agency in the Nation immediately begin or continue their efforts toward becoming Cyber Mature by implementing a methodology to determine the location of key assets, supply chain dependences where interruptions could compromise core law enforcement activities, and identifying threats within the context of a risk management framework.

-The Protect Core Function. Protect ensures that critical services remain operational. Using the risk tolerances, asset information, and other details developed during the Identify function, a law enforcement agency can best determine how to create manage resources to ensure security and resilience. This includes both cybersecurity and physical security risks to cyber infrastructure as well as training, maintenance, and the creation of processes and procedures. The process of applying patches and updates is the most critical safeguard that law enforcement agencies can apply and should be considered by every U.S. law enforcement agency. Multifactor authentication is a secondary defense that provides a layered approach to network protection. Fulfilling the Protect Core Function by Continuous Network Monitoring involves inspection of every network packet entering or egressing a network, as well as inspection of system level activity for problematic threat characteristics. While equipment manufacturers are making progress toward this end, "Remote Continuous Monitoring" in which an experienced and currently informed Cyber SME conducts the effort remotely (e.g., via the Internet), is a service affordable to law enforcement agencies, and is clearly superior to any other approach, and should be considered by every U.S. law enforcement agency.

-The Detect Core Function. These capabilities enable an agency to detect and remediate threats residing on devices within the network. Although engaging a 24x7x365 cybersecurity team is out of reach for most law enforcement agencies, there are a variety of services and resources that will ensure events are detected and their impacts are understood. Many of these resources involve taking advantage of free resources provided through the Cybersecurity and Infrastructure

Security Agency (CISA) and/or the use of managed service providers. CISA maintains a list of free, recommended resources and tools here: https://www.cisa.gov/free-cybersecurity-services-and-tools. All U.S. law enforcement agencies have access to CISA resources, including the Multi-State Information Sharing and Analysis Center (MS-ISAC), to engage in services.
Given the lack of affordability to law enforcement of maintaining a physically present 24X7X365 Cybersecurity Team, delivering Real-Time Vulnerability Assessment services remotely (e.g., via the Internet) is clearly superior to any other approach, and should be considered by every U.S. law enforcement agency in the Nation.

-Cybersecurity "Respond" and "Recover" Core Functions
The "Respond" and "Recover" Core Functions become necessary once the Cyberdefense Core Functions have not achieved their purpose of defending the network against a serious cyber incident. Services to implement the Respond and Recover Core Functions are still out of financial reach for local law enforcement agencies although both CISA and MS-ISAC provide these services for free, to a varying extent, and some eservice providers can provide them remotely for an affordable fee for service. However, achieving Cyber Maturity, and the processes that entails, and purchasing Cyber Risk Insurance, are the best ways for U.S. local law enforcement agencies to minimize the financial impact of the occurrence of a serious cyber incident.

IN SUMMARY
To meaningfully address the Cyberthreat, we urge that every Sheriff, every local law enforcement agency head, and indeed, every Emergency Services Sector agency head, assure that his or her Cybersecurity Managers return to the Cybersecurity Fundamentals, as articulated In the NIST Cybersecurity Framework, and seek to address the NIST Cybersecurity Framework "Identify", "Protect" and "Detect" Core Functions. Vital Homeland Security and Hometown Security interests are at stake when the Critical Infrastructure represented by Sheriffs' Offices and Municipal Police Departments, and their partners in local law enforcement, do not put in place the Cybersecurity capabilities described in these three Core Functions.

IDENTIFIED POSSIBLE RESOURCES
Not every cybersecurity service provider provides services focused on putting in place the Cybersecurity measures described in the the NIST Cybersecurity Framework "Identify", "Protect" and "Detect" Core Functions. We have listed below several firms that, based on information and belief, provide services aimed at enabling their customers to fully meet the requirements of these three NIST Cybersecurity Framework Core Functions. We have included contact information for those firms.

- **CyberAndPrivacy.com, DEMYSTIFYING CYBER, PRIVACY, AND IT, https://cyberandprivacy.com/. https://cyberandprivacy.com/contact-us, 678-630-1307**
- **Tabiri Analytics, Inc., https://basinstreettech.com/securing-the-digital. Edwin Kairu, 716-249-1411**

- **Fireeye, https://www.fireeye.com/, Endpoint Security, Comprehensive endpoint defense to stop breaches in their tracks: The Trellix Platform, https://www.trellix.com/en-us/products.html. info@fireeye.com.**
- **Cydome, COMPLETE CYBER SECURITY AT SEA, https://cydome.io/. info@cydome.io.**

THE RECOMMENDED PATH FORWARD ON CYBERSECURITY FOR SHERIFFS & THEIR PARTNERS

PART 2: TO MEANINGFULLY ADDRESS THE CYBERSECURITY INSIDER THREAT, CYBERSECURITY MANAGERS MUST LOOK BEYOND TECHNICAL THREAT VECTORS, AND ALSO CONSIDER NON-TECHNICAL HUMAN BEHAVIORAL THREAT VECTORS.

BACKGROUND

Insider cyber-attacks are one of the most formidable cyber security risks within the law enforcement community. One Sheriff recently commented that he would rather have his software platform locked down with ransomware than have it divulged publicly.

The DHS Cyber and Infrastructure Security Agency (CISA) defines "insider threat" as the threat that an insider will use his or her authorized access, **wittingly or unwittingly**, to do harm to the System mission, resources, personnel, facilities, information, equipment, networks, or systems. Various statistics suggest that 25% to 60% of all cyber-attacks are "insider" cyber-attacks. The large range of 25% to 60% is based upon whether insider-attacks include all of the unintentional cyber phishing hacks from employees who are distracted, lack proper training, and/or lack enough sleep.

A global leader in physical security routinely invokes the following guidance:

STOP SECURITY INCIDENTS BEFORE THEY HAPPEN

Can local law enforcement leaders **STOP CYBERSECURITY INCIDENTS BEFORE THEY HAPPEN**? This Part 2 discusses how, at least with respect to the **intentional insider threat**, local law enforcement leaders, and their constituents, can do just that. However, to do that, they are going to need to be aware of the importance of the human behavioral aspect of security, and be open to upping their guard regarding those human behavioral aspects--factors which are outside the scope of technical cybersecurity measures that have traditionally been considered by most cybersecurity professionals.

THE INADVERTENT INSIDER THREAT: WHERE INTENT IS NOT THE DANGER

We know that humans can get tired and distracted and as such make foolish errors and/or omissions that make their systems vulnerable to attacks. "[A]ccording to the '2020 IBM X-Force® Threat Intelligence Index', inadvertent insider threats are the primary reason for the greater than 200% rise in the number of records breached in 2019 as compared to 2018."[6] So, the percentage of insider attacks could be considerably higher now, in 2022, as compared to 2019.

THE INTENTIONAL INSIDER THREAT: WHERE INTENT—BEHAVIOR—IS THE DANGER

[6] **IBM X-Force® Threat Intelligence Index, "Why Are Insider Threats Particularly Dangerous?"** (2020).

"In the 2016 Cyber Security Intelligence Index, IBM found that 60% of all attacks were carried out by insiders. Of these attacks, three-quarters involved malicious intent, and one-quarter involved inadvertent actors.[7]"

Over the years, members of this Work Group have consulted with a number of Cybersecurity experts, and almost all have expressed the desire to prevent these intentional insider cyber-attacks by better understanding the "human behavior" of an attacker, and more specifically the ability to identify the behavioral precursors of an intentional cyber-attacker. Doing so requires avoiding the possible breach of privacy regulations such as HIPAA in our hospitals and healthcare facilities, FERPA on our campuses, and of course, the Civil Rights Act of 1964. Ensuring privacy regulation compliance while preventing insider cyber-attacks is especially important for Sheriffs and local law enforcement offices and personnel.

In trying to prevent insiders' intentional cyber attacks, experience has shown that the traditional approach of "See Something, Say Something" is not scientifically reliable. In large part, this may be because humans are not prepared to put their reputations or their jobs on the line, based upon subjective references. Also, subjective references have proven to be too often unreliable and anecdotal. Over the past years, members of this Work Group have searched for more predictive, scientifically reliable, objective, empirical and forensically measurable references.

IDENTIFY BEHAVIORAL PRECURSORS AND PREVENT INTENTIONAL INSIDER CYBER-ATTACKS?
Too often, the concept of "Security," in the context of cybersecurity, becomes a question of "how to thwart an attack that has already begun." However, we focused on identifying the "Precursors" to an attack, which offers an opportunity to prevent the attack in the first place. We found this to be not only a very innovative approach, but also a novel approach.

Accordingly, some time ago, members of this Work Group began looking for a system, as described by our cybersecurity experts, that could provide the human behaviors of an attacker, and more specifically the ability to identify the **behavioral precursors** of an insider who is or may be or become an intentional cyber-attacker. Logically, these precursors must also identify the "intent to do harm," such as the intent to do harm to a Sheriffs' Office's mission, resources, personnel, facilities, information, equipment, networks, or systems.

To truly be an effective law enforcement system, such a system must be science-based, intuitive enough to be useable by sworn personnel on the street, and include real-time observations of objective human body language, behavior and communication indicators. Furthermore, it must avoid the possible breach of privacy regulations. If the precursors used are too subjective, or too controversial due to the use of culture, gender, age, education, sexual orientation, or religion, Deputies simply won't use them. We also wanted to avoid the use of mental health assessments because they are not practical in the hands of

[7] **Harvard Business Review, "The Biggest Cybersecurity Threats Are Inside Your Company"** Marc van Zadelhoff, September 19, 2016.

everyday users such as Sheriffs' Deputies and police officers, and, even in the hands of mental health professionals, these assessments have been notoriously inaccurate.[8]

Considering the findings described above (**CISA, Cyber Security Intelligence Index**, and the **2020 IBM X-Force Threat Intelligence Index**), we sought to find systems that could identify someone who was trusted in the past, but who has become disgruntled or compromised, and is now **wittingly, with an intent to do harm,** moving toward treachery. Additionally, we also wanted a system to identify someone who, due to distractions, lack of training or lack of sleep, **will unwittingly** do harm to the department's mission, resources, personnel, facilities, information, equipment, networks, or systems.

FACTORS TO CONSIDER IN IDENTIFYING POSSIBLE SOLUTIONS

Finding a system that can do all of the above has been challenging. Most systems today use elements of mental health assessments, which are too subjective and may possibly violate HIPAA regulations; and/or use elements of culture, gender, age, education, sexual orientation, or religion, which violate FERPA on our school campuses, as well as the Civil Rights Act of 1964. These detractions make these programs and systems unreliable for use by all law enforcement agencies, including Sheriffs and Municipal Police Chiefs. Very few vendors offer services that have the ability to identify someone who has an "intent to do harm" to others.

IDENTIFIED POSSIBLE RESOURCES

We have listed below several resources that have an "insider threat" capability, and have provided contact information for those firms. As behavioral aspects are outside the scope of most cybersecurity service providers, these organizations operate well outside the scope of services of traditional Cybersecurity Service Providers:

- **Center for Aggression Management, Inc., "Critical Aggression Prevention System (CAPS)," 11956, Iselle Drive, Orlando, FL 32827, 407-718-5637, https://aggressionmanagement.com/index.php**
- **ONITC, "Manage and investigate insider threats," 4009 Marathon Blvd., Austin, TX 78756, 512-572-7400, https://ontic.co/**
- **AT-RISK International LLC, "Insider Threat Program Development," 14100 Parke Long Ct, Chantilly, VA 20151, (703) 378-2444, https://at-riskinternational.com/**

[8] Seung-Hui Cho (Virginia Tech Shooter) was mental health-assessed three times and, on each occasion, was deemed to be "depressed and anxious, but not a risk of hurting himself or others." See **Wall Street Journal, Gunman's Evaluations Didn't Foresee Frenzy**, Aug. 20, 2009.
Nikolas Cruz (Parkland Shooter) was mental health-assessed by the Florida Department of Children and Families and was deemed to be not "at risk of hurting himself or others." See **Washington Post, Red flags: The troubled path of accused Parkland shooter Nikolas Cruz**, March 10, 2018.

THE RECOMMENDED PATH FORWARD ON CYBERSECURITY FOR SHERIFFS & THEIR PARTNERS

PART 3: TO MEANINGFULLY ADDRESS THE CYBERTHREAT, LOCAL LAW ENFORCEMENT CYBERSECURITY MANAGERS MUST LOOK BEYOND TRADITIONAL LOCAL LAW ENFORCEMENT ORGANIZATIONAL BOUNDARIES, AND FIND AND IMPLEMENT NEW CYBERSECURITY APPROACHES THAT WORK IN THE REAL WORLD.

BACKGROUND

After living with an increasingly visible cyberthreat for at least five years now, it is clear that the cyberthreat is not going away any time soon. It is also clear that Cybersecurity is not a luxury that Sheriffs, their local law enforcement partners, or indeed, any agency in the Emergency Services Sector, can ignore, any more than they can ignore physical security measures necessary to protect their personnel, the assets under their control, or the citizens whom they have been sworn to protect and serve.

At the same time, the task of protecting a local Office or Department against the Cyberthreat is well beyond the capabilities and resource capacity of the vast majority of the local law enforcement agencies in the United States. What path forward, then, exists for the vast majority of local law enforcement agencies in the U.S.?

CYBERSECURITY: A SPECIALIZED DISCIPLINE VERY DIFFERENT FROM IT ADMINISTRATION

It is highly relevant to note here that the discipline of cybersecurity is an entirely separate discipline—involving somewhat related but very different knowledge bases and skillsets than are involved in the discipline of Information Technology Administration. In today's world, then, no local law enforcement leader can, within the obligations of their Oath, blindly rely on their IT Staff to assure that their agency is adequately protected against the cyberthreat, or blindly pretend that inadequate resources are an acceptable excuse for failing to protect their agencies from the cyberthreat.

CONSIDER THE ALTERNATIVES

Many under-resourced local agency leaders do what they can do within very constrained financial resources: they build a record of a) requesting adequate resources to mount a meaningful cyber defense through their budgeting processes, and b) seeking quotes from responsible service providers who can provide a meaningful cyberdefense. To these possibilities, we urge local law enforcement and other ESS agency leaders to consider creating or assembling an alternative for cybersecurity/cyberdefense which is within their agency's financial constraints.

THE COLORADO OIT MODEL

Since most local law enforcement agencies have extremely limited budgets for cybersecurity/cyberdefense, and because the cybersecurity challenge is still new, there have been few models for such alternatives. The Work Group, however, has become aware of a model that local law enforcement agencies, and, indeed, every agency within the Emergency Service Sector, should actively consider. That model has been carried out by the State of Colorado

Governor's Office of Information Technology ("CO OIT"), https://oit.colorado.gov/, and is referred to as "ReimagineIT", the "State of Colorado IT Transformation Program" (the "CO Program").[9]

Mr. Anthony Neal-Graves, Colorado's Chief Information Officer & Executive Director of the Governor's Office of Information Technology leads the CO OIT and the CO Program, and Mr. Ray Yepes, Colorado's Chief Information Security Officer (CISO), a Member of this Work Group, has key responsibilities for the CO OIT and the CO Program.

STATE OR REGIONAL GOVERNMENTAL CYBERSECURITY SERVICE PROVIDER ALTERNATIVES

In essence, the CO OIT and the CO Program are State governmental initiatives that provide, among other things, Cybersecurity Services for Colorado agencies as their "Customers". Operating under the premise that the cyberthreat is not going away any time soon, the Nation's Sheriffs should consider the alternatives for outsourcing their cybersecurity service needs to a governmental agency in their own States.

For example, it may be possible and of interest for some of the Sheriffs' Offices and Municipal Police Departments in a State to outsource their cybersecurity service needs to a State agency such as CO OIT. Alternatively, multiple Sheriff's Offices and Police Departments in a given state may be able to form an entity like a Joint Powers Authority[10] in California, to provide services meeting the cybersecurity service needs of the State's local law enforcement agencies.

IN SUM

To meaningfully address the cyberthreat, we urge local law enforcement leaders to look beyond traditional law enforcement organizational boundaries, and find and implement cybersecurity solutions that work in the real world.

We urge that Sheriffs and local law enforcement leaders nationally consider outsourcing key cybersecurity functions to work in coordination with the agency's IT staff. Outsourcing alternatives include private contractors, some of which may be more affordable than you think. Alternatively, State and regional law enforcement associations may want to consider requesting that state government take on the cybersecurity function for the state's local law enforcement

[9] For additional information, see **State of Colorado, IT Transformation Program, Two-Year Report, August 2020-August 2022,** https://drive.google.com/file/d/1Ec2g1ScjGrczivxDGuq4R7fZw5NVxNqw/view?usp=sharing.

[10] A joint powers authority is "a legally created entity that allows two or more public agencies to jointly exercise common powers", **see Paula C.P. de Sousa Mills, The Ins and Outs of Joint Powers Authorities in California (Jan. 14, 2016),** https://www.bbklaw.com/news-events/insights/2016/authored-articles/01/the-ins-and-outs-of-joint-powers-authorities-in-ca.

agencies, or, as another alternative, local law enforcement agencies may want to consider forming a multi-agency authority akin to a Joint Powers Authority to perform that function.

IDENTIFIED POSSIBLE RESOURCES

The following Work Group Members have expressed willingness to speak with Sheriffs and their local law enforcement parties about the alternatives for meeting their cybersecurity obligations:

- **Mr. Ray Yepes, Chief Information Security Officer (CISO), State of Colorado, 832-465-2377, or ray.yepes@state.co.us**
- **Sheriff David Goad (Ret), Past NSA President, 301-268-2901 or dgoad78@gmail.com**
- **Dennis Kelly, Esq., General Counsel, Basin Street Technologies, Inc. and Work Group Vice Chair, 504-251-0240 or dkelly@basinstreettech.com**

ACKNOWLEDGMENTS

The NSA Cybersecurity & Crime Work Group, under the leadership of Sheriff David Goad, wishes to acknowledge the material contributions to this Report provided by a number of law enforcement and cybersecurity professionals who are Members or Supporters of the Work Group.

The Work Group expresses special thanks to the following: Dr. William Bertrand, former Chief Information Officer, Tulane University; Edwin Kairu, CEO, Tabiri Analytics, Inc.; Dr. John Byrnes, CEO, Center for Aggression Management, Inc.; Ms. Stacey Wright, CISSP, Work Group Executive Committee; Dennis Kelly, Esq., General Counsel, Basin Street Technologies, Inc. and Work Group Vice Chair; and, of course, Sheriff David Goad, Past NSA President and Work Group Chair.

####