State, Local, Tribal, and Territorial Information Sharing Program: Pilot Project Overview

Fiscal Years 2019 and 2020

July 8, 2022

Fiscal Year 2022 Report to Congress

Homeland Security

Cybersecurity and Infrastructure Security Agency

Message from the Director

July 8, 2022

I am pleased to present the following report, "State, Local, Tribal, and Territorial Information Sharing Program: Pilot Project Overview" for Fiscal Years (FY) 2019 and 2020, which has been prepared by the Cybersecurity and Infrastructure Security Agency (CISA).

This document has been compiled pursuant to Senate Report 115-283, which accompanies the FY 2019 Department of Homeland Security (DHS) Appropriations Act (P.L. 116-6); and Senate Report 116-125, which accompanies the FY 2020 DHS Appropriations Act (P.L. 116-93). Included is an overview.

Pursuant to congressional requirements, this document is being provided to the following Members of Congress:

The Honorable Lucille Roybal-Allard
Chairwoman, House Appropriations Subcommittee on Homeland Security

The Honorable Chuck Fleischmann
Ranking Member, House Appropriations Subcommittee on Homeland Security

The Honorable Christopher S. Murphy
Chair, Senate Appropriations Subcommittee on Homeland Security

The Honorable Shelley Moore Capito
Ranking Member, Senate Appropriations Subcommittee on Homeland Security

Inquiries relating to this report may be directed to CISA Legislative Affairs at (202) 819-2612.

Sincerely,

Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency

Executive Summary

CISA established the State, Local, Tribal, and Territorial (SLTT) Information Sharing Program to foster a more resilient SLTT cyber ecosystem. Cooperative agreements were awarded in accordance with congressional direction to meet the project objectives set by CISA and to execute the project using a standardized process. Each pilot project includes the development of deliverables (e.g., guidance documents, best practices) that SLTT governments can adopt to meet their unique needs and constraints.

The Joint Explanatory Statement accompanying the FY 2019 DHS Appropriations Act (P.L. 116- 6) directs CISA to provide a report on the results of a pilot program to explore and evaluate the most effective methods for cybersecurity information sharing. In 2019, the Johns Hopkins University Applied Physics Laboratory (JHU/APL) was awarded $1,986,791 to pilot ways to apply automation to enhance the speed and evaluation of cyber-threat indicators of compromise (IOC) at the state and local government levels. In 2020, the same laboratory was awarded an additional $500,000 to develop a series of white papers, job aids, visual aids, and technical demonstrations to translate the findings of the initial project to foster greater adoption of security automation and to drive implementation of automation concepts for critical infrastructure. During the entire life of the project, which lasted 23 months, JHU/APL successfully met every objective of the pilot program and ultimately provided guidance on how SLTT agencies can act upon IOCs within minutes of receipt, dramatically reducing review time. The report titled "State, Local, Tribal, and Territorial Cyber Information Sharing Program: Pilot Project Overview Fiscal Years 2018, 2019, and 2020," issued in March 2021, detailed the findings of Year 1. Those findings are included in this report along with new updated findings from the second year to provide a wholistic view of the project's successes.

In 2019, the Cybercrime Support Network (CSN) was awarded a cooperative agreement in the amount of $999,981 to pilot the SLTT Reporting and Threat Information Sharing Pilot. In 2020, CSN was awarded $625,000 as a follow-on noncompetitive continuation to pilot cyber incident reporting, data analysis, and information-sharing processes and structures with SLTT governments. During the 27-month project, CSN sought ways to provide SLTT support to individuals and small businesses and explored considerations to improve reporting of cyber incidents nationally. CSN met the pilot's objectives and key performance metrics, successfully piloting a reporting structure and releasing the Victim Resource Catalog.

State, Local, Tribal, and Territorial Information Sharing Program: Pilot Project Overview Fiscal Years 2019 and 2020

Table of Contents

I. Legislative Language

Senate Report 115-283, which accompanies the Fiscal Year (FY) 2019 Department of Homeland Security (DHS) Appropriations Act (P.L. 116-6), states:

> *Cyber Readiness and Response*. —Of the total provided, $3,000,000 is for the continuation of pilot programs to explore and evaluate the most effective methods for cybersecurity information sharing, focusing on regional information sharing; communications and outreach; training and education; and research and development for the improvement of SLTT government capabilities, and capacity. NPPD is directed to provide a report on the results of each pilot not later than 270 days after its completion.

Senate Report 116-125, which accompanies the FY 2020 DHS Appropriations Act (P.L. 116-93), states:

> *Regional Information Sharing*. —Of the total provided, $3,000,000 is recommended to award grants or cooperative agreements to sustain or conduct new pilot programs to explore and evaluate the most effective methods for cybersecurity information sharing, focusing on regional information sharing; communications and outreach; training and education; and research and development for the improvement of SLTT government capabilities, and capacity. CISA is directed to provide a report on the results of each pilot not later than 180 days after its completion.

II. Background

The Cybersecurity and Infrastructure Security Agency (CISA), formerly named the National Protection and Programs Directorate, or NPPD, works with partners to defend against today's threats and to collaborate to build a more secure and resilient infrastructure for the future. CISA is at the heart of mobilizing a collective defense as it leads the Nation's efforts to understand and manage risk to its critical infrastructure and associated National Critical Functions.

CISA's partners in this mission span the public and private sectors, and the programs and services that CISA provides are driven by its comprehensive understanding of the risk environment and the corresponding needs identified by its stakeholders. CISA seeks to help organizations to manage risk better and to increase resilience using all available resources, whether provided by the Federal Government, commercial vendors, or their own capabilities.

CISA builds the national capacity to defend against cyberattacks and works with the Federal Government to provide cybersecurity tools, incident response services, and assessment capabilities to safeguard the ".gov" networks that support the essential operations of partner departments and agencies.

CISA also coordinates security and resilience efforts using trusted partnerships across the private and public sectors and delivers technical assistance and assessments to federal stakeholders as well as to infrastructure owners and operators nationwide. In addition, CISA delivers insights on these assessments related to current capabilities to identify gaps, which—along with an examination of emerging technologies—help to determine the demand for future capabilities (both near- and long-term).

CISA enhances public safety interoperable communications at all levels of government to help partners across the country to develop their emergency communications capabilities. Working with stakeholders across the country, CISA conducts extensive, nationwide outreach to support and promote the ability of emergency response providers and relevant government officials to continue to communicate in the event of a natural disaster, act of terrorism, or other man-made disaster.

III. CISA's State, Local, Tribal, and Territorial Information Sharing Program

Established in 2018, the CISA State, Local, Tribal, and Territorial (SLTT) Cyber Information Sharing Program conducts individual pilots to evaluate ways to improve cyber information sharing with and between SLTT agencies. CISA identifies critical issues facing the SLTT community and conducts individual, short-term (12 to 24 months) projects to pilot solutions. Cooperative agreements are awarded to a variety of organizations, each with specialized abilities to meet the unique requirements of each pilot. The findings are used to develop guidance documents, best practices, key considerations, models, processes, and procedures that SLTT agencies can adapt and modify to fit their resource constraints and operational needs. This effort provides tested solutions that SLTT agencies can apply themselves.

This is part of a self-service approach whereby findings are shared nationally so that SLTT agencies can apply them as they see fit. The layered approach complements direct assistance provided by CISA and indirect assistance that CISA sponsors via the Multi-State Information Sharing and Analysis Center (MS-ISAC). The information derived from individual pilot projects also informs products and services provided by CISA and MS-ISAC.

On March 8, 2021, CISA reported to Congress on the SLTT Cyber Information Sharing Program overview for FY 2018, 2019, and 2020. Pursuant to Senate Report 115-283, the report outlined the results of the FY 2019 SLTT Indicators of Compromise (IOC) Automation and the SLTT Reporting and Threat Information Sharing Pilots. This report is being submitted to fulfill the FY 2020 Congressional reporting requirements. The scope of this report is Year 2 of the SLTT IOC Automation Pilot Project.

IV. Analysis of Completed Pilot Projects

The following section summarizes the completed pilot projects, and provides an analysis of findings and considerations for the two pilots completed during FY 2019 and 2020—the SLTT IOC Automation Pilot and the SLTT Reporting and Threat Information Sharing Pilot.

SLTT IOC Automation Pilot

Overview

In September 2019, through a competitive process, CISA awarded a 1-year cooperative agreement to the Johns Hopkins University Applied Physics Laboratory (JHU/APL) and continued the cooperative agreement 1 additional year through August 31, 2021. The first cooperative agreement was awarded for $1,986,791 with a 1-year period of performance from September 30, 2019, to September 30, 2020. The second cooperative agreement was awarded for $500,000 as a noncompeting continuation with a performance period of September 30, 2020, to August 31, 2021. Funds were expended following the guidelines provided in the notice of the cooperative agreement award.

Purpose

The purpose of the pilot project was to apply automation to enhance and speed the evaluation of threat IOCs at the state and local government levels. In addition, the pilot identified key areas for potential reduction of manual tasks and improved actionable information sharing across enterprises and SLTT agencies. The pilot also identified orchestration services needed to integrate the activities of sensing, understanding, decision-making, and acting.

The pilot project focused on developing model processes, methods, and accompanying policies and procedures that can be applied by SLTT agencies to accomplish the following:

- Act upon IOCs within minutes of receipt;
- Reduce the time spent on repetitive tasks;
- Provide generation, enrichment, and IOCs scoring;
- Receive, remediate, and respond to IOCs;
- Demonstrate the use of Security Orchestration, Automation, and Response (SOAR) operational procedures and capabilities combined with information sharing to make data more actionable and to enable consistent execution across SLTT levels; and
- Develop repeatable processes for orchestration and automation services that bridge existing SLTT policies with SOAR capabilities.

CISA and JHU/APL selected and conducted the pilot project with four SLTT organizations:

- State of Arizona (Department of Administration and Maricopa County);
- State of Louisiana (Division of Administration);

- Commonwealth of Massachusetts (Executive Office of Technology Services and Security); and
- State of Texas (Department of Information Resources and Department of Public Safety).

CISA and JHU/APL also partnered with MS-ISAC to develop a network-defender threat intelligence feed to export indicators from the pilot feed in Structured Threat Integration Expression/Trusted Automated Exchange of Intelligence Information format and to use SOAR platforms to respond to those indicators of four state partners with different architectures and operational procedures. The pilot focused on both the curation of the feed as well as the processes used by the SLTT participants to triage, prioritize, and act upon the resulting IOCs.

Security Automation and Orchestration Metrics and Measures

The following tables provide insight into metrics and measures for the pilot project to determine how Security Automation and Orchestration capabilities and techniques introduce benefits, value, and effects. The pilot metrics offer insights for how Security Automation and Orchestration has been applied, on efficiencies gained, on cyber security operations effectiveness, and on an overall return on investment. Metrics and measures focused in four primary categories:

- Operational Performance – Evaluate and recognize Security Automation and Orchestration value, benefits, issues, and effects as they relate to security operations and performance.
- Systems Performance – Evaluate and recognize value, issues, and effects as they relate to cybersecurity practices and Security Automation and Orchestration support.
- Process Performance – Evaluate and recognize value, issues, and effects as they relate to organizational practices and process dependencies that directly impact Security Automation and Orchestration value.
- Workflow Execution – Assist organizations to design, develop, monitor, tune, troubleshoot, and maintain Security Automation and Orchestration capabilities.

The following describes the specific measures for each category.

Table 1: Operational Performance Measures and Metrics

Measure/Metric	Description	Rationale/Utility
1. Mean time to notification	Time between a potential malicious activity detected and an alert is provided to the person or system responsible for investigating	· Summarize operational value when compared with prior practices
2. Mean time to investigation	Once an alert has been sent, how much time passes before the investigation begins and what the duration of the investigation is	· Throughput · Summarize operational value · Ability to handle higher volumes of investigations, alerts, and data
3. Mean time to remediation	Total elapsed time from alert to investigation to remediation	· Summarize operational value · If organization is achieving quicker detection and response
4. Remediation summary statistics	Statistics tracking manual, semi-automated and automated remediation	· Characterize the level of automation applied in operations · Track progression for each type of remediation
5. Percent Investigated vs. Alert Volume	Investigations vs. alert volume	· Security Operations risk gap
6. Performance Improvements	Information collected to show how automation is improving processes and resource utilization	· Operational value in terms of performance · Resource savings

Table 2: System Performance measures and metrics

Measure/Metric	Description	Rationale/Utility
1. Workflow utility	Track how many incidents and types of incidents were aided by workflows	· Utilization trends · Operational value for incident and alert triage · Operational practices and dependencies
2. Sensor utilization	Track playbook/workflow dependencies on sensors, threat feeds and data sources	· Potential impact of compromised or unavailable sensor(s) · Heavily vs. underutilized sensor(s) · Which sensors aid investigation and/or remediation actions
3. Sensor value	Track which sensors, threat feeds and data (sources) aided an investigation or remediation	· Potential impact of compromised or unavailable sensor(s)

		· High-valued vs. underutilized sensor(s) · Sensor tuning effectiveness · Which sensors aid investigation and/or remediation actions
4. Threat Indicator	Track which threat indicator(s) aided an investigation or remediation	· Types and sources of indicators aiding security operations
5. Queued workflows or actions	Number of playbooks, workflows, investigations queued	· Ability to scale and support demand · Identify system bottlenecks · Throughput · System failures
6. Concurrency/Parallel workflows	Number of playbooks, workflows or investigations executed per time period	· Ability to scale and support demand
7. Workflow interface dependencies	Track which product integration interfaces were used in or are required for workflow execution	· Security infrastructure dependencies · Common, duplicative vs. purposely separated system interfaces
8. Performance Degradation	Information collected to show how automated processes are impacting system or process performance negatively	· Counterproductive operational impact
9. Custom Measures	Enable admin. and users to create and save measures or calculations for use in analysis	· Performance measures and key performance indicators differ by organization, culture, and goals. Offer the flexibility for organizations to define and analyze performance and results.

Table 3: Process Performance Measures and Metrics

Measure/Metric	Description	Rational/Utility
1. External process dependencies	Identifies workflows that have a dependency on an external process or system	· Operational dependencies across organizations, systems, tools, and practitioners
2. Workflows requiring human intervention	Track playbook/workflow dependencies on human interaction	· Workflows that require an approval or human interaction as part of execution · Workflows that can execute without human interaction · Classifying how different types of workflows may

		benefit by manual or automated validation, verification, and/or audit
3. Workflow effectiveness	Track which workflows were effective for their intended goal vs. required additional investigation or analysis	· Poorly defined processes that cannot be automated consistently · Opportunities to enhance workflows and to reduce manual processing required · Additional sensors, sources and/or analysis techniques relevant to the task
4. Analyst/Practitioner/ Organization interactions	Track which organizations and staff were required to interact with a workflow to facilitate an end goal; track within and across connected workflows	· Organizational dependencies · Opportunities to streamline operations across organizations · Inform service level agreements between organizations

Table 4: Workflow Execution Measures and Metrics

Measure/Metric	Description	Rational/Utility
1. Frequency of workflow revisions	Statistics tracking the frequency of workflow/playbook revisions	· Stability of workflows · Complexity of workflows · Audit authorized and verified changes · Automated tests to verify and validate results and intent
2. Frequency of workflow execution	Statistics tracking the frequency of workflow/playbook execution	· Potential impact to operations if compromised or unavailable · Frequency of initiating condition or alerts
3. Frequency of remediation actions taken	Statistics tracking the frequency of actions taken to remediate threats/risks	· Audit changes made to operational assets · Frequency of changes made to certain operational assets
4. Workflow utilization	Track how many times a workflow is selected manually vs. automated and runs	· Utilization trends · Operational practices and dependencies
5. Workflow value	Savings estimate by multiplying the cost of performing repetitive tasks manually by the estimated number of times the system performs those tasks	· Estimated time and/or cost savings · Return on investment

	automatically during a specific date/time range	
6. Workflow confidence level	Statistics tracking the frequency automated recommendations are confirmed for execution	· Confidence in semi-automated/automated course of action recommendations · Potential workflows to enhance with automation
7. Workflow idle time	Statistics tracking times that workflows were paused waiting for data, a decision, action, or approval	· Efficiency opportunities for processes and workflows · Throughput/efficiency constraints · Sources of bottlenecks
8. Workflow reliability	Track successful vs. unsuccessful executions (success, failure, error rates)	· Reliability trends · Failures common across workflows
9. Workflow decision processing	Capture triggering condition, key values/decision points, and end state	· Verify that certain actions are taken if, and only if, certain conditions are true
10. Workflow dwell time	Statistics tracking workflow execution times	· Performance (typical vs. abnormal) · Change in system or capabilities
11. Workflow deployment readiness	Evidence verifying and validating that workflows are defined by compliant practices and that they execute as intended	· Workflow dependencies · If workflows can be verified, audited, and validated

CISA exercised substantial programmatic involvement throughout the cooperative agreement. This included monitoring project progress; providing technical assistance; disapproving and approving subprojects, workplans, or modifications thereto; holding kickoff meetings; and conducting programmatic reviews. The DHS Grants and Financial Assistance Division oversaw the execution of the grant based on input from CISA, discussion with the awardee, and through the Program Performance Reporting Requirements.

In April 2021, the DHS Grants and Financial Assistance Division completed a desk audit review of the pilot, which included an assessment of JHU/APL's award-related management policies, a review of the accounting and financial system practices, and a review of the award cash management procedures for calculating draw-down amounts. Based on the Grants and Financial Assistance Division's review of the information provided, there were no significant findings identified.

JHU/APL successfully met every objective of the pilot as specified by CISA and collected all data available for the analysis of metrics requested in the notice of funding opportunity.

Pilot Overview

In its first year, the pilot identified key areas for potential reduction of manual tasks and orchestration services needed to integrate the activities of sensing, understanding, decision-making, and acting with respect to cyber threats.

To achieve the SLTT IOC Automation Pilot objectives, CISA and JHU/APL used a four-phased approach:

- Discovery Phase - select pilot partners and identify the pilot scope;
- Design Phase - collaborate with pilot partners and create pilot workflows;
- Execution Phase - implement pilot technology on partner production networks and collect data; and
- Analysis and Reporting Phase - analyze and report the findings of the pilot.

During the discovery phase, with CISA concurrence, JHU/APL evaluated and selected Arizona, Louisiana, and Texas as the SLTT IOC Automation Pilot partners. After an assessment of the funding level, Massachusetts was considered and selected for a single security use case using an orchestration proof-of-concept, given its current manual process. All state partners, as well as MS-ISAC, have consented to participate as the threat feed providers. Preliminary discussions and site visits were held in order to ascertain pilot environments and to determine the scope for each pilot partner.

During the design phase of the pilot, JHU/APL worked closely with multiple SLTT agencies and MS-ISAC to understand their current procedures. They developed an automated MS-ISAC threat feed as well as automated responses to IOCs from that threat feed. The design phase documented the proposed automated responses in shareable workflow form.

During the execution phase of the pilot, JHU/APL worked closely with multiple SLTT agencies and MS-ISAC to provide consultation and guidance to integrate the pilot technology in the partner environments and to assist each partner with execution of the pilot plan.

Pilot participants included:

- State of Arizona (Department of Administration and Maricopa County),
- Commonwealth of Massachusetts (Executive Office of Technology Services and Security),
- State of Louisiana (Division of Administration), and
- State of Texas (Department of Information Resources and Department of Public Safety).

This effort led to successful integration of pilot capability with multiple members of the SLTT community and has allowed for the collection of data necessary to evaluate the core metrics of this pilot effort.

The analysis and reporting phase of the pilot discovered that a majority of SLTT organizational participants planned to continue their use of SOAR, and security automation based on their

experiences with this pilot. Many of the participants have begun to research and develop expanded-use cases to leverage the capability identified in the pilot. Additionally, several members looked to expand similar capability from the pilot either within their states or to provide examples for other states interested in using SOAR.

CISA and JHU/APL had to: select candidates from the MS-ISAC SLTT member community, create a new feed for threat intelligence, identify a transition partner for the feed, develop six enterprise security integration environments, create dozens of workflows, and transition those workflows as well as the feed to operations. To accomplish this successfully, a threat-feed provider and four SLTT partners were needed.

The first objective of the pilot was to demonstrate the ability to act upon IOCs within minutes of receipt. The automation at MS-ISAC receives IOCs from intrusion detection system alerts as well as submissions to the Malicious Code Analysis Platform. Once received, the pilot automation processes these IOCs within an average time of 42 seconds and distributes them to the pilot Trusted Automated Exchange of Intelligence Information server within an additional 30 seconds. Therefore, action not only was initiated, but was completed in just more than 1 minute. Once an SLTT pilot partner received an IOC from the Trusted Automated Exchange of Intelligence Information feed, the automated actions began, on average, within 2 seconds of receipt and on average, took a total of 98 seconds to complete. The automation can provide IOCs rapidly, instead of as a weekly publication. The SLTT organization then had the opportunity to block potential cyberattacks proactively before an adversary could pivot to target the organization.

The second objective was to reduce the time spent on repetitive tasks. The pilot performance demonstrated a substantial reduction in the time spent on repetitive tasks. There was a reduction in the overall process from 4,086 minutes to 3 minutes when comparing the manual and automated processes. This was because of automation that can run in the background, not requiring humans to complete repetitive tasks during their workweek. Even factoring in the substantial amount of time spent on waiting for a human to review an automated prompt, the pilot still demonstrated more than an eightfold speed improvement over the manual process.

The third objective, through the creation of the pilot threat feed, was to generate, enrich, and score the IOCs. The threat feed produced for the SLTT IOC Automation Pilot Project was a completely new set of IOCs derived from MS-ISAC data using a low-regret strategy. This unique strategy was based on determining the likelihood of operational impact to an organization if it responds to an IOC. The regret determination and sharing processes were automated fully, and the score provided was used by the receiving sites to determine response actions in an automated fashion.

The fourth objective was to develop workflows for SLTT partner organizations to receive, remediate, and respond to IOCs. The primary method of response to an IOC was to block the IOC. IOCs received by SLTT partners were blocked, but 99 percent of the IOCs had no history on the network and thus were safe to block without disrupting operations. This meant that, although the low-regret nature of the feed was preserved, the pilot partners were still able to

maintain control of their own policy and chose only to block IOCs that they could confirm as truly malicious.

The fifth and final objective of the pilot was the successful deployment of SOAR workflows with four states using various platforms across the SOAR marketspace. Each of the pilot states had a favorable response to the use of SOAR and looks to continue usage of the technology.

***Year 2* of the pilot provided outreach guidance and analysis reports learned from the insights discovered during Year 1 of the pilot.**

JHU/APL was granted a follow-on tasking under the cooperative agreement to provide outreach guidance and analysis reports learned from the insights discovered during Year 1 of the pilot. To further the goals of the pilot, continuation funding was used to expand the adoption of security automation, the pilot threat feed, and the implementation of automation concepts. The key public deliverables translated the successes and lessons learned from the core pilot effort into easily understandable artifacts for the SLTT community. The overall objective was to translate the findings of the Year 1 grant effort and to leverage the lessons learned into a series of white papers, job aids, visual aids, and technical demonstrations.

Year 2 Pilot Project Deliverables

The SOAR workflows delivered through Year 1 of the project allowed the SLTT members of the pilot program to design and tailor their own SOAR workflows rapidly for the pilot use cases. To expand upon this offering for all other members of critical infrastructure, the grantee developed a repository of approximately 50 SOAR workflows that were both vendor-agnostic and shareable in a public forum. A set of 30 additional workflows from the pilot were included as an example set of how to tailor various workflows. All 80 SOAR workflows were reassessed publicly and were made available via CISA's page on GitHub. Building on the efforts in Year 1, Year 2 efforts focused on developing guidance and documents to help SLTT agencies to understand and implement SOAR.

Topic-Specific White Paper Series and Instructional Videos
It was determined that a set of best practice documents were needed in both usage of SOAR and the sharing of cyber-threat intelligence to amplify the success of the pilot effort. In order to share these insights with the community, the grantee created an 11-part white paper series to convey the findings to the public. The white papers are available at https://www.cisa.gov/state-local-tribal-territorial-cyber-information-sharing-program and include the following topics:

- *Assessing the Potential Value of Cyber Threat Intelligence Feeds*. The paper describes how an organization can assess a product, service, or cyber threat intelligence feed and associated cost to ascertain what solution best aligns with the organization's requirements.

- *Sharing Indicators of Compromise Network Defense – Operational Value of Indicators of Compromise*. The paper provides insights on what operational value some IOCs

provide to organizations, since threat actors can and do change IOCs routinely as a way to avoid detection.

- *Service Models for Cyber Threat Intelligence – Intelligence, Enrichment and Brokering as a Service*. The paper describes the types of cyber-threat intelligence products and services on the market.

- *Cyber Threat Intelligence Sharing Infrastructures - Preserving Cyber Threat Intelligence Content*. The paper describes design elements of cyber-threat intelligence standards such as Structured Threat Information Expression to ensure that the data sent is the data received.

- *Enabling Automation in Security Operations – Assessing Automation Potential of Products and Services*. How to assess products and services, those already deployed as well as those under consideration, to determine if they have limited automation potential.

- *Enabling Automation in Security Operations – Strategies for Efficient Process Automation*. The basic approach identified in this guide is to help an organization to develop and deploy automation that is more efficient and effective for their operations.

- *Enabling Automation in Security Operations - Increasing Automation Potential of Processes*. The best practices identified in this guide will help organizations to identify ways to make their processes and associated information management practices more conducive to cybersecurity orchestration.

- *Applying "Low-Regret" Methodology for Cyber Threat Intelligence Triage – Rapidly Sharing Actionable Intelligence for Network Defense*. In this paper, the methodology and process are provided in more detail to help organizations to leverage automation capabilities for their communities' network defense needs.

- *Applying "Low-Regret" Methodology for Response to Indicators - Rapidly Mitigating Indicators of Compromises at Scale*. This paper showcases how to apply a "low-regret" methodology for rapid evaluation and response to these IOCs via SOAR tools.

- *Cybersecurity Orchestration - Orchestration of Information Technology Automation Frameworks*. This paper defines what it means to orchestrate information technology automation frameworks.

- *Cybersecurity Orchestration - Information-Centric Automation and Orchestration*. This paper describes how automation and orchestration continues to evolve, and how organizations begin investing in information-centric operations from product-centric integration.

- *Low–Regret Instructional Videos*. One of the key concepts behind the success of the pilot was the application of the "low-regret" methodology for scoring cyber IOCs and design of response workflows. While there were two white papers on these topics,

additional demonstrations of how to apply this methodology were helpful to foster adoption within the community. Toward that goal, two instructional videos on the concept were produced and can be found on YouTube. The first video provides a high-level summary of the low-regret concept (found at https://youtu.be/gXt-iReKuVM). The second provides a more detailed set of technical demonstrations for employing the methodology (https://youtu.be/_-XvJ0UbqRk).

Analysis to Support CISA Security Automation and Cyber-Threat Information-Sharing Products and Services

In addition to the documents described above, the grantee developed a series of technical analyses for CISA's internal use with respect to security automation and cyber-threat intelligence-sharing products and services in support of SLTT organizations. The technical documents are described below.

- *Feasibility Study for Applying Low-Regret to CISA's Automated Indicator Sharing Feed.* During the pilot, the key factor in enabling significant improvement for cyber defensive operations was the creation of a "low-regret" scoring algorithm to evaluate IOCs from intrusion detection systems and to share that data within minutes, as opposed to legacy manual procedures that took days. This algorithm was applied to data from MS-ISAC, which saw a dramatic improvement in making an IOC feed actionable. Given that CISA provides the Automated Indicator Sharing feed for both public and federal consumers, there was interest in knowing if this approach could be a viable capability to integrate with the Automated Indicator Sharing feed. Thus, CISA asked if JHU/APL could apply the same approach to IOCs shared via the Automated Indicator Sharing feed. Based on the analysis conducted in this study, the JHU/APL did not recommend that CISA apply the regret scoring methodology to the Automated Indicator Sharing feed in its current form. The characteristics of the IOCs and the lack of any consistent context to support the regret determination process negated the potential value associated with a "low-regret" feed of indicators derived from the Automated Indicator Sharing feed.

- *Insights into Information Sharing Infrastructure*. This paper discusses operational insights, both organizational and technical, gathered during the pilot. JHU/APL analyzed certain aspects of the pilot feed infrastructure in order to identify key elements that enabled it to provide the observed benefits seen in the pilot activity. As a result, a number of challenges were observed across SLTT organizations. These challenges ranged from technical to organizational culture and access issues. In general, organizations struggle to process the flood of information to determine what cyber-threat intelligence is relevant to them, to use what is shared to make appropriate mitigation decisions in a timely manner, or to contribute threat insights back to the community.

- *Concepts on Building Trust in Automation*. This paper expanded upon the grantee's research and development of the Trust in Automation Framework. The Trust in Automation Framework accounts for factors contributing toward trust in automation with the goal of helping cyber analysts understand how human behaviors, attitudes, and perception of automation in their workspace affects their ability to calibrate their level of

trust and reliance on automation correctly, as well as their perception of the automated system's trustworthiness.

Promoting Adoption by State and Local

The initial pilot project results briefings were provided to each of the following SLTT participants and to the MS-ISAC:

- State of Arizona (Department of Administration and Maricopa County)
- Commonwealth of Massachusetts (Executive Office of Technology Services and Security)
- State of Louisiana (Division of Administration)
- State of Texas (Department of Information Resources and Department of Public Safety)

These briefings provided overall pilot findings, as well as specific insights into pilot performance with the specific participant. Results were provided to each participant, as was a customized written report.

The state and local participants and MS–ISAC are planning to continue their use of SOAR and security automation based on their experiences with this pilot. Many already have begun to research and develop expanded-use cases to leverage the capability identified in the pilot. Additionally, pilot participants members are looking to expand similar capability from the pilot either within their states or to provide examples for other states interested in using SOAR.

The grantee participated in multiple conferences, webinars, and technical exchanges with information sharing and analysis centers (ISAC), as well as in other fora for critical infrastructure partners to share the pilot results. The following is a summary of the key briefings and technical exchanges:

- Aviation ISACs: Technical exchange to determine what aspects of the pilot could benefit the ISACs.
- Downstream Natural Gas ISAC: Provided a summary briefing on the pilot accomplishments to members through a monthly webinar.
- Health ISAC Summit: Provided a briefing on the pilot results and a briefing on the needs for an advanced cyber-threat information-sharing ecosystem.
- National Council of Information Sharing and Analysis Centers: Provided a summary briefing on the pilot accomplishments to approximately 20 ISACs.
- Research and Education Network ISAC annual member meeting: Provided a summary briefing of pilot results.
- Western Governors Association: Participated in a panel discussion on the needs of states for defense against advanced cyber threats.

Lessons Learned

Use of SOAR

The pilot proved to be overwhelmingly successful in speeding up the evaluation of IOCs and in increasing dramatically the ability of pilot participants to protect their networks from potentially malicious activity. Furthermore, the participants will continue to use SOAR and security automation. Participants already have begun to research and develop expanded-use cases to leverage the capability identified in the pilot. Additionally, several participants are looking to expand the use of the capability from the pilot either within their states or to provide examples for other states interested in using SOAR. Also, MS-ISAC found distinct value in the automated low-regret feed of IOCs and has transitioned the technology into a production offering.

Technical Challenges

There were some technical challenges leveraging Trusted Automated Exchange of Intelligence Information clients and servers. None of the pilot partners had much experience using Trusted Automated Exchange of Intelligence Information for the retrieval of IOCs from MS-ISAC. When investigating vendor-based tools, CISA and JHU/APL discovered that critical structured threat information expression fields from the IOCs with respect to the regret score were overwritten by the vendor without notification. The use of separate polling scripts and command line-based clients became necessary to ensure that partners received the threat intelligence feed with all the information needed. Although the pilot provided documentation to support the use of these tools, the added documentation placed a significant burden on the Security Operations Center staff MS-ISAC utilizing Trusted Automated Exchange of Intelligence Information. Alternative distribution methods for IOCs may be needed to make information more accessible to the greater SLTT community.

Product Version Control

The number of data sources, products, and services deployed in enterprise environments continues to increase, as does the number of these capabilities used by Security Operations Center personnel to perform different functions (e.g., investigation, remediation). Maintaining accurate insight into the current versions, functionality, licensing restrictions, and organization-wide usage is not a simple matter, especially when different parts of the organization manage different resources and different aspects of the lifecycle for a resource. Every pilot partner had at least one product or service identified for a use case that was either the wrong version, was unable to provide the necessary feature/function in an automated manner, violated vendor usage restrictions, or did not support local policies properly as encoded in the workflow. The results determined how critical it is for every organization investing in SOAR capabilities to have up-to-date information about their resource accessed as part of an automated workflow to include exact versions, licensing restrictions, local policy/usage restrictions, and application programming interface functionality. It is also important to consider the ability to automate (e.g., application programming interface functionality, integration support) as part of the procurement/acquisition process for external products/services and the requirements/development process for internal products and applications.

Automation Process Workflows

The SLTT IOC Automation Pilot represented different levels of interactions with existing processes at different partner locations. In some cases, completely new processes were designed and implemented. In most, existing manual processes were automated, and a ticketing or tracking tool was used to manage the touchpoints between new tasks and current operations. In every case, a significant amount of time was spent in understanding the current state and in

designing the automation to ensure minimal negative impact to ongoing operations and manageable interactions with operators. As organizations implement automation and orchestration in their environments, they need to make sure that there is a plan to implement, monitor, refine, and extend these automation workflows. In particular, organizations need to ensure that deployment and testing/validation do not have a negative impact on existing operations/operators and that extended automation does not require a redesign of the workflow. Essentially, it is recommended to build with the expectation of full automation and then to add simple touchpoints using existing capabilities whenever possible.

Consideration

CISA works with SLTT governments to promote the adoption of common policies and best practices that are risk-based and are able to respond effectively to the pace of ever-changing threats. Through this initiative, CISA received a considerable number of deliverables and insight from the pilot project and is providing sample workflows, best practice white papers, videos, and guides to assist SLTT governments as well as to other members of the critical infrastructure community that are using or considering SOAR to automate their cybersecurity operations. Recognizing that SOAR is an advanced capability that not all SLTT governments will be able to adopt immediately, the intention of the pilot project is threefold: 1) provide resources to SLTT governments that are ready to implement or procure such services; 2) provide planning considerations for SLTT governments to consider for future action; and 3) initiate a conversation with the broader cybersecurity community on where we should be moving.

SLTT Reporting and Threat Information Sharing Pilot

Overview

In FY 2019, CISA awarded a new cooperative agreement titled "State, Local, Tribal, and Territorial Reporting and Threat Information Sharing Pilot." The cooperative agreement supports the implementation of the Homeland Security Act of 2002, as amended by the Cybersecurity and Infrastructure Security Agency Act of 2018, specifically providing shared situational awareness to enable real-time, integrated, and operational actions across the Federal Government and nonfederal entities to address cybersecurity risks and incidents.

Purpose

The purpose of the SLTT Reporting and Threat Information Sharing Pilot project was to provide SLTT organizations with greater visibility of cyber-threats affecting their communities and to allow law enforcement agencies to respond to otherwise unreported cyber incidents. The pilot's intent was to use an advance nationwide cyber incident "2-1-1" SLTT capability and to respond to cyber incidents by standardizing the reporting structure and mechanism. Also, the pilot project would identify a standardized list of resources that could be provided to SLTT organizations and victims of cyber incidents.

In September 2019, through an open and competitive process, CISA awarded a 1-year cooperative agreement totaling $999,981 to the Cybercrime Support Network (CSN). The cooperative agreement was extended for 11 months via a post-award amendment through August 31, 2021, at no additional cost. Year 2 of the cooperative agreement was awarded a noncompeting continuation for $625,000 with a performance period of September 30, 2020, to August 31, 2021. A 4-month no-cost extension enabled completion of the pilot following the approval of the SLTT Incident Collection under the Paperwork Reduction Act, extending the period of performance through December 31, 2021. All of Years 1 and 2 funds were expended following the guidelines provided in the notice of the cooperative agreement award.

CISA used the following criteria to evaluate applicants deemed eligible and responsive:

- Capacity to provide leadership in identification and development of an SLTT reporting and threat information-sharing platform that will be used to advance nationwide cyber incident "2-1-1" SLTT capabilities and efforts to respond to cyber incidents by standardizing the reporting structure, mechanism, and available resources;
- Capacity to develop documentation including design, policies and procedures, concept of operations, and operational manuals;
- Capacity to provide wide outreach;
- Cost-effectiveness and balance.

In doing so, CSN established a team consisting of the following partners:

Cybercrime Support Network
CSN is a public-private, nonprofit collaboration created to meet the challenges facing millions of individuals and businesses affected each and every day by cybercrime. CSN works with national partners and law enforcement to bring real, actionable solutions to victims of cybercrime. CSN's mission is to improve the plight of Americans facing the ever-growing impact of cybercrime by bringing together national partners to support cybercrime victims.

The Center for Internet Security (CIS)
CIS partnered with CSN to facilitate the SLTT Threat Information Sharing and Reporting Pilot project. CIS operates the MS-ISAC and the Elections Infrastructure ISAC, which currently combines services to more than 8,700 SLTT government members. CIS was able to engage communities rapidly because of its far-reaching relationship to the SLTT community.

National Strategic Planning and Analysis Research Center (NSPARC)
NSPARC partnered with the grantee on the pilot to develop and implement an online incident collection form. As a top-tier research institution and a CISA Center of Excellence for Cybersecurity, NSPARC is a trusted partner with government entities and also across the private and public sectors.

Aspen Institute
The grantee partnered with the Aspen Institute to study the online reporting form's usability. The Aspen Institute earned a reputation for gathering diverse, nonpartisan thought leaders, creatives, scholars, and members of the public to address some of the world's most complex problems.

Performance Metrics

The key performance parameters for measuring the effectiveness during the performance period are shown below.

Table 5: Performance Measures and Metrics

Performance Measures/Metrics	**Performance Objectives**	
Measures	*Threshold*	*Objective*
Prototype Reporting Structure	1-2	2
Develop support documentation (e.g., designs, policies and procedures, concept of operations, and operations manual(s), etc.)	1-2	2
Pilot prototype	1-2	2
Strategic Plan	1	1
Feasibility Study of National Resource List	1	1
Lesson Learned Reports	2-4	2
National-Level Feasibility Study	1	1

CISA exercised substantial programmatic involvement through this cooperative agreement. This included quarterly monitoring of project progress; providing technical assistance; holding kickoff

meetings; and conducting biannual and programmatic reviews. The DHS Grants and Financial Assistance Division oversaw the execution of the cooperative agreement and the overall performance of the grantee from an administrative and financial perspective. The pilot accomplishments were executed at or below budgeted levels in every area.

All funds were expended following the guidelines provided in the notice of the cooperative agreement award.

In April 2021, the DHS Grants and Financial Assistance Division completed a desk audit review of the pilot that included an assessment of CSN's award-related management policies, a review of the accounting and financial system practices, and a review of the award cash management procedures for calculating draw-down amount. Based on the Grants Office review of the information provided, there were no significant findings.

Objectives

The objectives of the SLTT Reporting and Threat Information Sharing Pilot:

- *Objective One:* Utilizing the nationwide "2-1-1" or similar infrastructure, develop a prototype cyber incident reporting network with a nexus to law enforcement.
- *Objective Two:* Develop documentation including design, policies and procedures, concept of operations, and operations manual(s) for a national-level cyber incident reporting program, to include defining the scope of what types of cyber incidents would be addressed.
- *Objective Three:* Pilot the reporting structure with a select number of SLTT organizations.
- *Objective Four:* Study the feasibility to build and maintain a national list of cybersecurity resources based on location and incident type that SLTT entities can offer to victims.
- *Objective Five:* Study the feasibility for a national-level program.
- *Objective Six:* Document lessons learned and levels of efforts.

Deliverables

The following describes the deliverables and work accomplished to meet each objective.

Objective One: Identifying which existing "2-1-1" or similar infrastructure to leverage during the course of this pilot. In the end, CISA and the grantee agreed on an information-sharing approach that leveraged the existing infrastructure of CIS to share incident trend reports safely and effectively to stakeholders. To do this, the grantee worked with NSPARC and the Aspen Institute to incorporate recommendations from prior research on the study of the online reporting form's usability. Visitors to FightCybercrime.org from the pilot states of Michigan, Mississippi, North Carolina, Rhode Island, and Utah were presented with the option of reporting cyber incidents through a user-friendly online form developed by the pilot. State law enforcement agencies in those states received individual cyber incident reports, along with analysis of monthly cyber incident trends in their respective state. Additionally, the grantee developed a report for tracking trends of different types of cyber incidents based on traffic patterns on

FightCybercrime.org. SLTT agencies received trend reports via CIS accompanied by educational resources and outreach aids for public consumption each month during the pilot.

Objectives Two: The Incident-Based Pilot included the development of incident report handling processes, trend report development processes, software designs to support incident report collection, processing, dissemination, trend report generation, and accompanying process documentation and guides.

Objective Three: The grantee established a series of criteria to ensure that the pilot participating states would provide useful insight into cyber threats affecting individuals and small businesses. Two criteria categories were developed: first, a series of threshold requirements that would be applied to all pilot partners as prerequisites, and second, a series of overall requirements that would ensure a balanced or "diverse" pilot partner set. After meeting the selection criteria, the states of Michigan, North Carolina, Rhode Island, Mississippi, and Utah were identified and confirmed to participate in the pilot. Fusion centers and other organizations within the pilot states also were identified and confirmed. Over a 5-month period, CSN piloted the Incident Collect Form with the five pilot states. As part of the pilots, the following were developed:

- **Cyber Resources Request Reports** highlight the changes in individuals and small businesses' interests in resource assistance dealing with different types of cyber incidents at both national and state-specific levels (for five pilot states), as well as the procedures and tools necessary to produce the numerical analysis in the report.
- **Cyber Resources Request Trend Reports** detail the changing interests of individuals and small businesses in resource assistance with different types of cyber incidents at both national and state-specific levels.

Objective Four: The pilot approached this objective to build a national list of cybersecurity resources by first developing a gap analysis and two surveys to gather data regarding the utility and purpose of a Response Directory and a Victim Resource Catalog. The surveys provided valuable insight that not only offered practical guidance for the pilot, but also reaffirmed the mission and objective of the pilot. The survey to study the needs and feasibility for a nationwide Response Directory was completed in Year 1. The pilot therefore combined the Response Directory objectives into the related Victim Resource Catalog efforts. The pilot collected existing resources, produced an extensive amount of new educational materials, and developed a user-searchable Victim Resource Catalog. The following resources also were developed:

- **Cyber Resources and Cyber Outreach Aids** include information for individuals and small businesses about recognizing, reporting, recovering from, and reinforcing preventative measures against cyber incidents identified as of significant interest based on Cyber Resources Request Reports trends.
- **Web-hosted Cyber Resources Catalog** of more than 1,000 cyber resources suitable for SLTT agencies support to individuals and small businesses.
- **Gap Analysis of resources** needed by, but unavailable to, individuals and small businesses that have been affected by cyber incidents.

Objective Five: As part of the cooperative agreement, the pilot delivered a study that assessed the feasibility of a national-level program. The results of the SLTT Reporting and Threat Information

Sharing Pilot indicate that a national program to support SLTT entities and individuals and small businesses with cyber resilience, reporting, and recovery is feasible to implement.

Objective Six: Part two of the feasibility study describes lessons learned from the pilot to include design, policies, procedures, and concepts of operation. The feasibility study is one of the pilot deliverables.

- **Feasibility Study Part 1** analyzed the current state of cyber information-sharing among SLTT agencies and support for individuals and small businesses.
- **Feasibility Study Part 2** documented lessons learned from the SLTT Cyber Information Pilot and potential implications for a national-level program.
- **Functional Plan** identified and evaluated alternative approaches for a national program supporting SLTT efforts to improve the cyber resilience of individuals and small businesses.

Lessons Learned

Website Analytics-Based Approach
The pilot identified advantages in using analytical techniques that do not depend on formal reports of individual cyber incidents to increase visibility into cyber incident trends affecting individuals and small businesses. The website analytics-based approach produced a much greater volume of data from which to identify trends than did the collection of individual cyber incident reports in pilot states. Further, collecting individual cyber incident reports involved regulatory, infrastructure, and interface management costs that the website analytics-based approached avoided. Website analytics show great promise for individuals and small business cyber trend analysis, especially if improvements are made to increase data collection and accuracy.

State-by-State Incident-Based Approach
The approach employed in the Incident-Based Pilot to share individual cyber incident reports on a state-by-state basis faces significant hurdles at a national scale, including the high cost of establishing interfaces with each organization and the limited capacity of SLTT law enforcement agencies to handle increased incident report volumes. Leveraging existing CIS infrastructure to handle the receipt of personal and sensitive data accelerated the technical delivery of the individual cyber incident report collection.

Cyber Resilience Resources with Encouragement to Report Incidents
The pilot found that SLTT agencies' commitment in helping their individuals and small business constituents with resources could be an effective partnership in greatly expanding cyber risk awareness and resilience. Several SLTT pilot participants involved in addressing cyber issues indicated that public outreach was a significant part, perhaps even the most time-consuming part, of their jobs. This was especially true of SLTT law enforcement agencies whose representatives explained that they prioritized limited resources for raising public awareness over investigating cyber incidents, which often exceeded their legal jurisdictions.

The pilot found that coupling cyber resilience resources with encouragement to report

incidents, simplifying the reporting process, and making it easier to report attempted (but unsuccessful) cyber incidents could help to increase law enforcement awareness of specific cyber threats to individuals and small businesses. Following adjustments to FightCybercrime.org to make it easier for site visitors to navigate to cyber incident reporting forms, between 8-9 percent of visitors to relevant pages clicked on links to do so; a much higher rate than some estimates of individuals affected by cyber incidents who choose to report and double the rate prior to the adjustments. Pilot results also suggest that some combination of form design (ease of use had been a key design parameter of the Incident Collection Form) and hosting the form on a nongovernment website contributed to a higher form completion rate than observed on existing government incident reporting forms.

SLTT Public Outreach.
Nearly 450 SLTT representatives signed up from a single outreach email when presented with an opportunity to subscribe to a toolkit with information about cyber trends affecting individuals and small businesses and resources to help educate their constituents. Of those, at least 37 downloaded at least one resource intended for public outreach. A representative from a state fusion center shared that the center assists many individuals and small businesses that call with cyber issues by pointing them to the resources on FightCybercrime.org. These results suggest that SLTT entities would benefit from an expanded, trusted library of resources to assist their individuals and small business constituents with cyber issues. The pilot results further suggest that it is important to partner with SLTT representatives in roles that involve public outreach.

Co-branding Cyber Resource Catalog
The pilot identified that stakeholders preferred a combined catalog of cyber resilience resources for individuals and small businesses rather than a separate catalog and directory for incident response organizations. Co-branding lent credibility to the resources in the Cyber Resource Catalog.

Considerations and Opportunities to Improve Cyber Resilience, Reporting, and Recovery

SLTT government support to individuals and small businesses remains a challenge, as individuals and small businesses rarely have the technical knowledge, skills, or resources to prepare for, respond to, and recover from cyber incidents. An abundance of resources and tools is available, ranging from traditional informational resources to incident reporting, data collection, and intelligence-sharing. SLTT agencies attempt to provide more detailed information for their jurisdictions, but the breadth, scope, and speed of cyber incidents challenge the experts to keep resources current and available.

The pilot identified four primary needs of SLTT entities in support of individuals and small businesses to address cyber issues. First, there is a need for quality informational resources about cyber threats and best practices to improve resilience to cyber risks. The pilot found that many SLTT entities offer such resources to their constituents today, but their availability and quality varies. Second, individuals and small businesses need help identifying trustworthy sources of assistance to recover from cyber incidents. The pilot found that SLTT entities lack the resources to provide or even recommend assistance. Third, SLTT entities need to understand what cyber risk and threats their constituents face so that they can prioritize services, resources,

and outreach effectively. The pilot found that little information about changing cyber trends was available to SLTT governments. Finally, there is a need for actual and attempted cyber incidents to be reported via an SLTT-designed mechanism to drive the understanding of trends and to enable effective responses. Against the background of the Russia-Ukraine war, public officials have warned that hacktivist groups may escalate their malicious cyber operations, which could (directly or indirectly) impact the United States and local businesses. The Cyber Incident Reporting for Critical Infrastructure Act of 2022 legislation was "designed to encourage compliance with the law, by describing the types of events that constitute a covered cyber incident for reporting purposes, increase the quantity and quality of cyber incident reporting," and will provide additional resources for SLTT governments. The SLTT Reporting and Threat Information Sharing Pilot project tested solutions to address each of the needs identified.

V. Conclusion

Through cooperative agreements, CISA is utilizing pilot projects to build capacity and to provide solutions to defend and protect against cyberattacks at the SLTT government level for a more resilient SLTT cyber ecosystem. The two pilots conducted under the SLTT Cyber Information Sharing Program have tested ways to improve cyber information-sharing with and between SLTT agencies. Executed by organizations with specialized abilities to meet the unique requirements of each pilot, the findings help the broader SLTT community to improve its capabilities. The pilots have produced guidance documents, best practices, resources, models, processes, and procedures that SLTT agencies can adapt and modify to fit their resource constraints and operational needs. More detailed reports with the outcomes of the two pilots can be found by visiting: cisa.gov/sltt-cyber-information-sharing-program. This effort provides CISA with the flexibility to develop tested solutions rapidly that SLTT agencies can apply themselves.

VI. Appendix: Abbreviations

Abbreviation	Definition
CISA	Cybersecurity and Infrastructure Security Agency
CIS	Center for Internet Security
CSN	Cybercrime Support Network
DHS	Department of Homeland Security
FY	Fiscal Year
IOC	Indicator of Compromise
ISAC	Information Sharing and Analysis Center
JHU/APL	Johns Hopkins University Applied Physics Laboratory
MS-ISAC	Multi-State Information Sharing and Analysis Center
NSPARC	National Strategic Planning and Analysis Research Center
NPPD	National Protection and Programs Directorate
SLTT	State, Local, Tribal, and Territorial
SOAR	Security Orchestration, Automation, and Response