United States Government Accountability Office

Report to Chair, Subcommittee on Emerging Threats and Spending Oversight, Committee on Homeland Security and Governmental Affairs, U.S. Senate

September 2022

RANSOMWARE

Federal Agencies Provide Useful Assistance but Can Improve Collaboration

GAO Highlights

Highlights of GAO-22-104767, a report to Chair, Subcommittee on Emerging Threats and Spending Oversight, Committee on Homeland Security and Governmental Affairs, U.S. Senate

Why GAO Did This Study

The Department of Homeland Security has reported that ransomware is a serious and growing threat to government operations at the federal, state, and local levels. In recent years, there have been numerous reported ransomware attacks on hospitals, schools, emergency services, and other industries.

GAO was asked to review federal efforts to provide ransomware prevention and response assistance to state, local, tribal, and territorial government organizations. Specifically, this report addresses
(1) how federal agencies assist these organizations in protecting their assets against ransomware attacks and in responding to related incidents,
(2) organizations' perspectives on ransomware assistance received from federal agencies, and (3) the extent to which federal agencies addressed key practices for effective collaboration when assisting these organizations.

GAO reviewed agency documentation from eight federal agencies to identify efforts to help state, local, tribal and territorial governments address ransomware threats. Documents reviewed included agency service catalogs, ransomware guidance, and agency websites. GAO supplemented these reviews with interviews of officials from CISA, FBI, Secret Service, Department of Justice, Federal Emergency Management Agency, Commerce's National Institute for Standards and Technology, and the Department of the Treasury.

For more information, contact David B. Hinchman at (214) 777-5719 or hinchmand@gao.gov.

September 2022

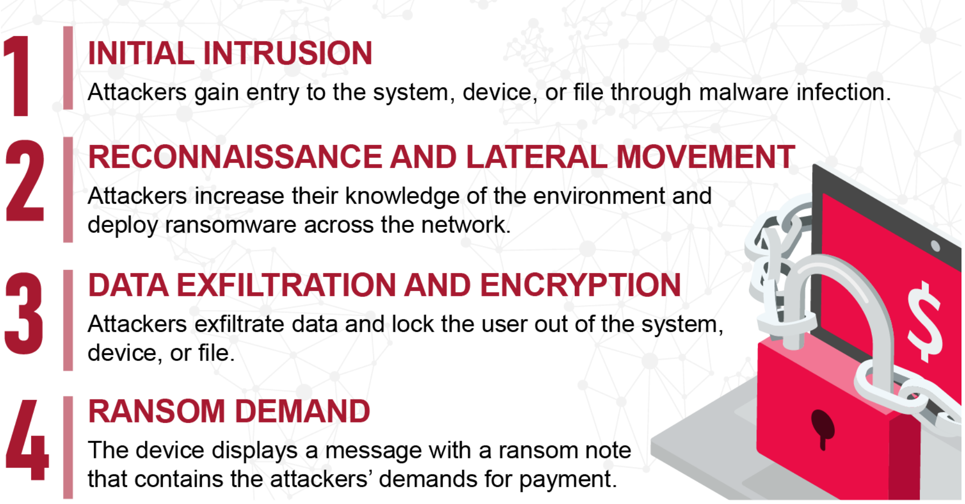
RANSOMWARE

Federal Agencies Provide Useful Assistance but Can Improve Collaboration

What GAO Found

Ransomware is a form of malicious software designed to encrypt files on a device and render data and systems unusable. Malicious actors then demand ransom payments in exchange for restoring access to the locked data and systems. A ransomware attack is not a single event but occurs in stages (see figure).

Figure: Four Stages of a Common Ransomware Attack


1 INITIAL INTRUSION
Attackers gain entry to the system, device, or file through malware infection.
2 RECONNAISSANCE AND LATERAL MOVEMENT
Attackers increase their knowledge of the environment and deploy ransomware across the network.
3 DATA EXFILTRATION AND ENCRYPTION
Attackers exfiltrate data and lock the user out of the system, device, or file.
4 RANSOM DEMAND
The device displays a message with a ransom note that contains the attackers' demands for payment.
$

Source: GAO analysis based on information from the Cybersecurity and Infrastructure Security Agency, Center for Internet Security, and Federal Bureau of Investigation; image: tomasknopp/stock.adobe.com. | GAO-22-104767

The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), FBI, and Secret Service provide assistance in preventing and responding to ransomware attacks on state, local, tribal, and territorial government organizations. For example:

- **Education and awareness.** CISA, in collaboration with FBI, Secret Service, and other federal partners, developed the www.stopransomware.gov website to provide a central location for ransomware guidance, alerts, advisories, and reports from federal agencies and partners.
- **Information sharing and analysis.** CISA, FBI, and Secret Service collect and analyze security and ransomware-related information—such as threat indicators, incident alerts, and vulnerability data—and share this information by issuing alerts and advisories. For example, CISA, through a cooperative agreement with the Multi-State Information Sharing and Analysis Center, provides intrusion detection sensors to nonfederal entities that reportedly analyze 1 trillion network activity reports per month.
- **Cybersecurity review and assessment.** CISA and the Multi-State Information Sharing and Analysis Center have provided review and assessment services upon request, such as vulnerability scanning, remote penetration testing, and risk assessments.

GAO also interviewed officials from government organizations receiving federal ransomware assistance who volunteered to share their perspectives. These officials represented governments from four states, eight localities, and one tribal nation. In addition, GAO interviewed officials from six national organizations. These groups included the National Governors Association; National League of Cities; National Association of State Chief Information Officers; and the National Association of State Auditors, Comptrollers, and Treasurers. To analyze responses from these interviews, GAO coded the qualitative data to enable identification of common trends across the interviews. The interview results from these interviews are not generalizable, but provide insight into perspectives on federal assistance in addressing ransomware.

GAO identified three federal agencies that provide direct ransomware assistance—CISA, FBI, and Secret Service—and assessed their efforts against key practices for interagency collaboration. To support its assessment, GAO reviewed agency documentation on collaborative mechanisms and efforts to coordinate assistance, such as joint alerts and guidance, incident coordination procedures, and interagency agreements. GAO also interviewed officials from the three agencies to clarify information about their collaborative efforts.

What GAO Recommends

GAO is making three recommendations to the Department of Homeland Security (CISA and Secret Service) and Department of Justice (FBI) to address identified challenges and incorporate key collaboration practices in delivering services to state, local, tribal, and territorial governments. The agencies concurred with GAO's recommendations.

- **Incident response.** When a ransomware attack occurs, CISA, FBI, and Secret Service can provide incident response assistance to nonfederal entities upon request. CISA and the Multi-State Information Sharing and Analysis Center provide technical assistance such as forensic analysis of the attack and recommended mitigations. Additionally, FBI and Secret Service primarily collect evidence to conduct criminal investigations and attribute attacks. According to the Multi-State Information Sharing and Analysis Center, state, local, tribal, and territorial governments experienced more than 2,800 ransomware incidents from January 2017 through March 2021.

Other federal agencies, such as the Federal Emergency Management Agency, National Guard Bureau, National Institute of Standards and Technology, and the Department of the Treasury have a more indirect role. These agencies provide ransomware assistance to nonfederal entities through administering cybersecurity grants, issuing guidance to manage ransomware risk, or pursuing sanctions to disrupt ransomware activity.

The officials from government organizations that GAO interviewed were generally satisfied with the prevention and response assistance provided by federal agencies. They had generally positive views on ransomware guidance, detailed threat alerts, quality no-cost technical assessments, and timely incident response assistance. However, respondents identified challenges related to awareness, outreach, and communication. For example, half of the respondents who worked with the FBI cited inconsistent communication as a challenge associated with the agency's ransomware assistance.

CISA, FBI, and Secret Service took steps to enhance interagency coordination through existing mechanisms—such as interagency detailees and field-level staff—and demonstrated coordination on a joint ransomware website, guidance, and alerts. However, the three agencies have not addressed aspects of six of seven key practices for interagency collaboration in their ransomware assistance to state, local, tribal, and territorial governments (see table).

Table: Extent to Which Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation, and Secret Service Addressed Key Collaboration Practices in Their Ransomware Assistance

Key practice	Extent addressed
Defining outcomes and monitoring accountability	Not addressed
Bridging organizational cultures	Partially addressed
Identifying and sustaining leadership	Generally addressed
Clarifying roles and responsibilities	Partially addressed
Including relevant participants	Partially addressed
Identifying and leveraging resources	Partially addressed
Developing and updating written guidance and agreements	Partially addressed

Source: GAO analysis of agency documentation. | GAO-22-104767

Specifically, the agencies generally addressed the practice of identifying leadership by designating agency leads for technical- and law enforcement-related ransomware response activities. However, the agencies could improve their efforts to address the other six practices. For instance, existing interagency collaboration on ransomware assistance to state, local, tribal, and territorial governments was informal and lacked detailed procedures.

Recognizing the importance of formalizing interagency coordination on ransomware, the *Consolidated Appropriations Act, 2022* required CISA to establish a Joint Ransomware Task Force, in partnership with other federal agencies. Among other responsibilities, the task force is intended to facilitate coordination and collaboration among federal entities and other relevant entities to improve federal actions against ransomware threats. Addressing key practices for interagency collaboration in concert with the new ransomware task force can help ensure effective delivery of ransomware assistance to state, local, tribal, and territorial governments.

Contents

Letter 1

Background 6
Federal Agencies Provide Ransomware Assistance to State, Local, Tribal, and Territorial Governments 20
SLTT Governments Were Generally Satisfied with Federal Ransomware Assistance, but Identified Challenges 36
Federal Agencies Partially Addressed Most Key Collaboration Practices 44
Conclusions 55
Recommendations for Executive Action 55
Agency Comments and Our Evaluation 56

Appendix I Comments from the Department of Homeland Security 59

Appendix II GAO Contacts and Staff Acknowledgments 64

Tables

Table 1: Products and Services That the Cybersecurity and Infrastructure Security Agency (CISA) Highlighted as Effective in Addressing State and Local Government Ransomware Threats 30
Table 2: Extent to Which Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation, and Secret Service Addressed Key Collaboration Practices in Their Ransomware Assistance to State and Local Governments 47

Figures

Figure 1: Four Stages of a Common Ransomware Attack 9
Figure 2: Types of Ransomware Assistance Available to State, Local, Tribal, and Territorial Organizations 22
Figure 3: Number of Enrollments in Cybersecurity and Infrastructure Security Agency's (CISA) Scanning and Testing Services 29

Abbreviations

CISA	Cybersecurity and Infrastructure Security Agency
DHS	Department of Homeland Security
DOJ	Department of Justice
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
IC3	Internet Crime Complaint Center
JCDC	Joint Cyber Defense Collaborative
K-12	kindergarten through grade 12
MS-ISAC	Multi-State Information Sharing and Analysis Center
NCIJTF	National Cyber Investigative Joint Task Force
NIST	National Institute of Standards and Technology
PPD-41	Presidential Policy Directive-41
Secret Service	United States Secret Service
SLTT	state, local, tribal, and territorial governments

GAO U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

September 14, 2022

The Honorable Margaret Wood Hassan
Chair
Subcommittee on Emerging Threats and Spending Oversight
Committee on Homeland Security and Governmental Affairs
United States Senate

Dear Madam Chair:

Ransomware, a type of malicious software used to force victims to make payments, is a serious and growing threat to government operations at the federal, state, and local levels. According to the Department of Homeland Security (DHS), attacks using ransomware have at least doubled since 2017.[1] In addition, the Multi-State Information Sharing and Analysis Center (MS-ISAC) found that state, local, tribal, and territorial (SLTT) governments experienced more than 2,800 ransomware incidents from January 2017 through March 2021.[2]

DHS's Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), the National Security Agency, and the cybersecurity authorities of Australia and the United Kingdom jointly reported in February 2022 that ransomware tactics and techniques continued to evolve in 2021. This demonstrates threat actors' growing technological sophistication and an increased threat to organizations at all levels.[3] In addition, CISA noted that malicious actors have continued to engage in ransomware attacks against state and local governments and small businesses.

[1] Department of Homeland Security, *Homeland Threat Assessment* (October 2020).

[2] The MS-ISAC is a division of the Center for Internet Security, an independent, nonprofit organization. The MS-ISAC was organized in 2002 to provide cyber threat information to state governments. Since fiscal year 2010, DHS has provided funding to the MS-ISAC through a cooperative agreement. The funding enables cyber threat information sharing and services to enhance SLTT governments' ability to prevent, protect against, respond to, and recover from cyberattacks and compromises.

[3] CISA, *2021 Trends Show Increased Globalized Threat of Ransomware,* Alert (AA22-040A) (Feb. 9, 2022), accessed Feb. 9, 2022, https://www.cisa.gov/uscert/ncas/alerts/aa22-040a.

We have previously reported that criminal groups are increasingly targeting U.S. critical infrastructure, which includes systems and assets supporting emergency services, government operations, elections infrastructure, telecommunications networks, and energy production and transmission facilities.[4] For example, in October 2021 we reported that when the COVID-19 pandemic forced the closure of schools across the nation, many kindergarten through grade 12 (K-12) schools moved from in-person to remote education.[5] This increased their dependence on IT and making them potentially more vulnerable to cyberattacks. We noted that schools have increasingly reported ransomware and other cyberattacks that can cause significant disruptions to school operations.

Given the increased trend in ransomware attacks across the nation, you asked us to review federal efforts to provide prevention and response assistance to SLTT government organizations. Specifically, this report addresses (1) how federal agencies assist SLTTs in protecting their assets against ransomware attacks and responding to related incidents, (2) SLTT governments' and national organizations' perspectives on ransomware assistance from federal agencies, and (3) the extent to which federal agencies addressed key practices for effective collaboration when providing ransomware assistance to SLTTs.

SLTT government organizations are part of the Government Facilities Sector, one of 16 critical infrastructure sectors. It includes government facilities owned and operated by the 56 states and territories, 3,031

[4] GAO, *High-Risk Series: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges,* GAO-21-288 (Washington, D.C.: Mar. 24, 2021); and *Election Security: DHS Plans Are Urgently Needed to Address Identified Challenges Before the 2020 Elections*, GAO-20-267 (Washington, D.C.: Feb. 6, 2020).

[5] GAO, *Critical Infrastructure Protection: Education Should Take Additional Steps to Help Protect K-12 Schools from Cyber Threats*, GAO-22-105024, (Washington, D.C.: Oct. 13, 2021).

counties, 85,973 local governments, and 574 federally recognized tribal nations.[6]

To address our first objective, we reviewed agency documentation from CISA, Department of Defense's National Guard Bureau, Department of Justice (DOJ), FBI, Federal Emergency Management Agency (FEMA), National Institute of Standards and Technology (NIST), United States Secret Service, and Department of the Treasury to identify federal efforts in helping SLTTs address ransomware threats. In doing so, we reviewed documentation such as agency service catalogs, ransomware guidance, agency websites, and internal reporting metrics on SLTTs' use of federally provided or funded products and services. We identified various ways that each agency provided assistance to SLTT governments and categorized the assistance as ransomware prevention or response. We developed subcategories to further break down prevention-related assistance as education and awareness, information sharing and analysis, or cybersecurity review and assessment.

To supplement our review of agency documentation, we also interviewed relevant federal officials regarding their agencies' roles in assisting SLTT officials in preventing and responding to ransomware incidents. Specifically, we interviewed headquarters officials from CISA, DOJ, FBI, FEMA, National Guard Bureau, NIST, Secret Service, and Treasury regarding ransomware assistance provided to SLTTs. We also interviewed officials from the Center for Internet Security, which operates the MS-ISAC in partnership with CISA, as a central resource for SLTTs to receive cybersecurity and ransomware-related services and information.[7]

To address our second objective, we conducted semi-structured interviews with officials from national organizations and SLTT governments to obtain perspectives on federal ransomware assistance efforts. Specifically, we interviewed officials from six national

[6] Our nation's critical infrastructure refers to the systems and assets, whether physical or virtual, so vital to the United States that their incapacity or destruction would have a debilitating impact on our nation's security, economic security, public health or safety, or any combination of these factors. Federal policy has identified 16 critical infrastructure sectors. In addition to the Government Facilities Sector, the other 15 sectors include: Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams; Defense Industrial Base; Emergency Services; Energy; Financial Services; Food and Agriculture; Healthcare and Public Health; Nuclear Reactors, Materials, and Waste; Information Technology; Transportation Systems; and Water and Wastewater Systems.

[7] CISA provides products and services to SLTT governments through a cooperative agreement with the MS-ISAC.

organizations that have SLTT membership or that have insight into cyber threats that SLTTs face: the Association of Local Government Auditors; National Association of State Auditors, Comptrollers, and Treasurers; National Association of State Chief Information Officers; National Conference of State Legislatures; National Governors Association; and National League of Cities.

Additionally, we interviewed officials from 13 SLTT governments to gain perspectives on the assistance they received from the federal government between January 2018 and May 2021. To identify the SLTTs we would interview, we solicited participation in our review through the National Association of State Chief Information Officers, National Governors Association, and MS-ISAC because those organizations had existing relationships with SLTTs and were providing ongoing guidance and support on cybersecurity issues at the state and local level. We interviewed all SLTTs that volunteered to share their experiences. Additionally, 12 of the 13 SLTTs we interviewed received ransomware prevention services from one or more federal agencies and 11 of the 13 SLTTs we interviewed received response assistance for a ransomware incident. The resulting 13 SLTTs represented four state governments, eight local governments, and one tribal government from a variety of population sizes and regions in the U.S.

We asked for SLTT officials' perspectives on federal ransomware assistance, such as services provided by federal agencies (e.g., risk and vulnerability assessments) or other assistance (e.g., guidance and best practices) intended to prevent a ransomware attack. We also discussed SLTT officials' perspectives on instances where they requested and received federal assistance in responding to ransomware incidents.

To analyze responses from SLTTs and national organizations, we systematically coded the qualitative data in order to identify common trends across the interviews. Specifically, we coded the relevant statements made in each documented interview using five general categories of responses such as service, awareness and outreach, satisfaction, interagency cooperation, and recommendation. We also used 15 unique subcategories to analyze and draw conclusions on the general themes, benefits, challenges, and improvement opportunities expressed by the national organizations and SLTTs we interviewed. For example, we coded statements as assistance related to education and awareness, information sharing and analysis, or review and assessment; an identified strength or weakness of the assistance provided; and lack of awareness of federal roles, services, and support available.

Prior to the coding process, we verified that the categories and their definitions were accurate, applicable, and clear. To do this, two analysts coded a sample of two interviews using the five categories and supporting subcategories to identify any inconsistencies and potential revisions to the categories or their definitions. Once we reviewed all of the responses from the interviewees using the categories, we had two analysts verify the coded statements. In addition, we interviewed officials from relevant federal agencies to gain additional perspectives on any existing or planned efforts that may address the challenges or improvement opportunities that SLTTs identified.

Due to the sensitivity of SLTTs' interactions with the federal government regarding the security of their systems and possible targeting for further victimization, we are providing information on national organizations' and SLTTs' perspectives in the aggregate. The results from these national organizations and SLTTs are not generalizable, but provide insight into perspectives on the federal government's efforts with ransomware.

To address our third objective, we evaluated coordination efforts of CISA, FBI, and Secret Service against seven key practices for interagency collaboration identified in our prior work.[8] We assessed these three agencies because they are the primary agencies federal guidance directs SLTTs to contact when requesting ransomware-related prevention and response services. We reviewed agency documentation from CISA, FBI, and Secret Service regarding the mechanisms they used to collaborate across agency boundaries and efforts to coordinate prevention and response assistance, such as joint alerts and guidance, incident coordination procedures, and interagency agreements.

We reviewed Presidential Policy Directive-41[9] on interagency collaboration for cyber incidents and we identified four principles as most relevant to the three federal agencies. The identified principles were

[8] GAO, *Managing for Results: Key Considerations for Implementing Interagency Collaborative Mechanisms,* GAO-12-1022 (Washington, D.C.: Sept. 27, 2012). For the purpose of this report we use the term "collaboration" broadly to include interagency activities that others have variously defined as "cooperation," "coordination," "integration," or "networking."

[9] The White House, *United States Cyber Incident Coordination*, Presidential Policy Directive/PPD-41 (Washington, D.C.: July 26, 2016). For the purpose of our review, we focused on the four principles we identified as most relevant to CISA, FBI, and Secret Service in providing ransomware assistance to SLTTs. These were identifying federal leads, coordinating agency response efforts, coordinating field-level activities, and establishing unified public communications.

consistent with the seven key practices for interagency collaboration used to assess each agency.

For each of the seven key practices for interagency collaboration, we identified documentation from each agency on mechanisms and other efforts to collaborate that were relevant to providing federal assistance to SLTTs on a ransomware incident, including general cyber incident coordination. We then made determinations about the extent to which the three agencies had generally addressed, partially addressed, or did not address applicable aspects of the key practices for interagency collaboration, based on the documentation and data provided. We also interviewed agency officials and interagency detailees[10] from CISA, FBI, and Secret Service who have been directly involved in providing ransomware support and assistance to SLTTs to clarify our understanding of agencies' adoption of key collaboration practices and to discuss their perspectives on how the agencies coordinate when providing assistance.

We conducted this performance audit from January 2021 to September 2022 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Ransomware is a form of malicious software designed to encrypt files on a device, rendering any data and systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. The ransomware perpetrators' can assert that if their demands are not met, the system or encrypted data will remain unavailable, data may be deleted, or the data could be released publicly. Alternatively, the perpetrators can assert if a ransom is paid, the victim will receive the information needed to regain access to the system or unencrypt the data.

Ransomware incidents can severely impact business processes and leave organizations without the data they need to operate and deliver mission critical services. According to CISA and MS-ISAC, malicious actors have adjusted their ransomware tactics over time to include

[10] For reporting purposes, interagency detailee includes non-reimbursable or reimbursable liaison officers and assignees designated to perform certain tasks at another agency while remaining employed by their home agency.

pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion. Malicious actors may also inform the victim’s partners, shareholders, or suppliers about the incident to further the damage to the business or existing relationships.[11]

For example, the FBI reported in September 2021 that cyber actors infected a U.S. county network with ransomware, resulting in the closure of the county courthouse and the theft of a substantial amount of county data (to include personal information on residents, employees, and vendors).[12] The county refused to pay the ransom and the actors posted the data on the dark web.[13]

The lack of access to state and local government organizations’[14] systems and data due to a ransomware attack can threaten critical services, such as health care, education, and emergency management.[15] According to Verizon, public safety agencies, including police departments, are considered easy targets because they have so much to lose to attacks that target sensitive data or lock down critical IT systems.[16] For example, the FBI reported that in January 2021, malicious actors infected local U.S. county government systems with ransomware

[11] CISA and MS-ISAC, “Ransomware Guide,” Ransomware Guide (2020), https://www.cisa.gov/stopransomware/ransomware-guide.

[12] FBI, Cyber Division, *Private Industry Notification: Ransomware Attacks Straining Local US Governments and Public Services*, Private Industry Notification 20220330-001 (Mar. 30, 2022).

[13] According to DOJ, the “dark web” refers to a part of the internet that cannot be accessed through standard web browsers but requires specific software, configurations, or authorization. Although many users access the dark web for legitimate purposes, because of the anonymity it provides it is also used for criminal activity, including drug trafficking and malware.

[14] For our review, we considered state governments to include components and agencies that provide services for the entire state (e.g., Texas Department of Transportation). We considered local governments to include components and agencies that provide services in a defined area, such as a county, city, town, borough, village, or township (e.g., St. Lucie County Sheriff’s Office).

[15] GAO, “Ransomware—Holding IT Systems and Data Hostage.” Web Blog. WatchBlog, June 30, 2021. https://www.gao.gov/blog/ransomware-holding-it-systems-and-data-hostage.

[16] Verizon, *2021 Data Breach Investigations Report*. https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/.

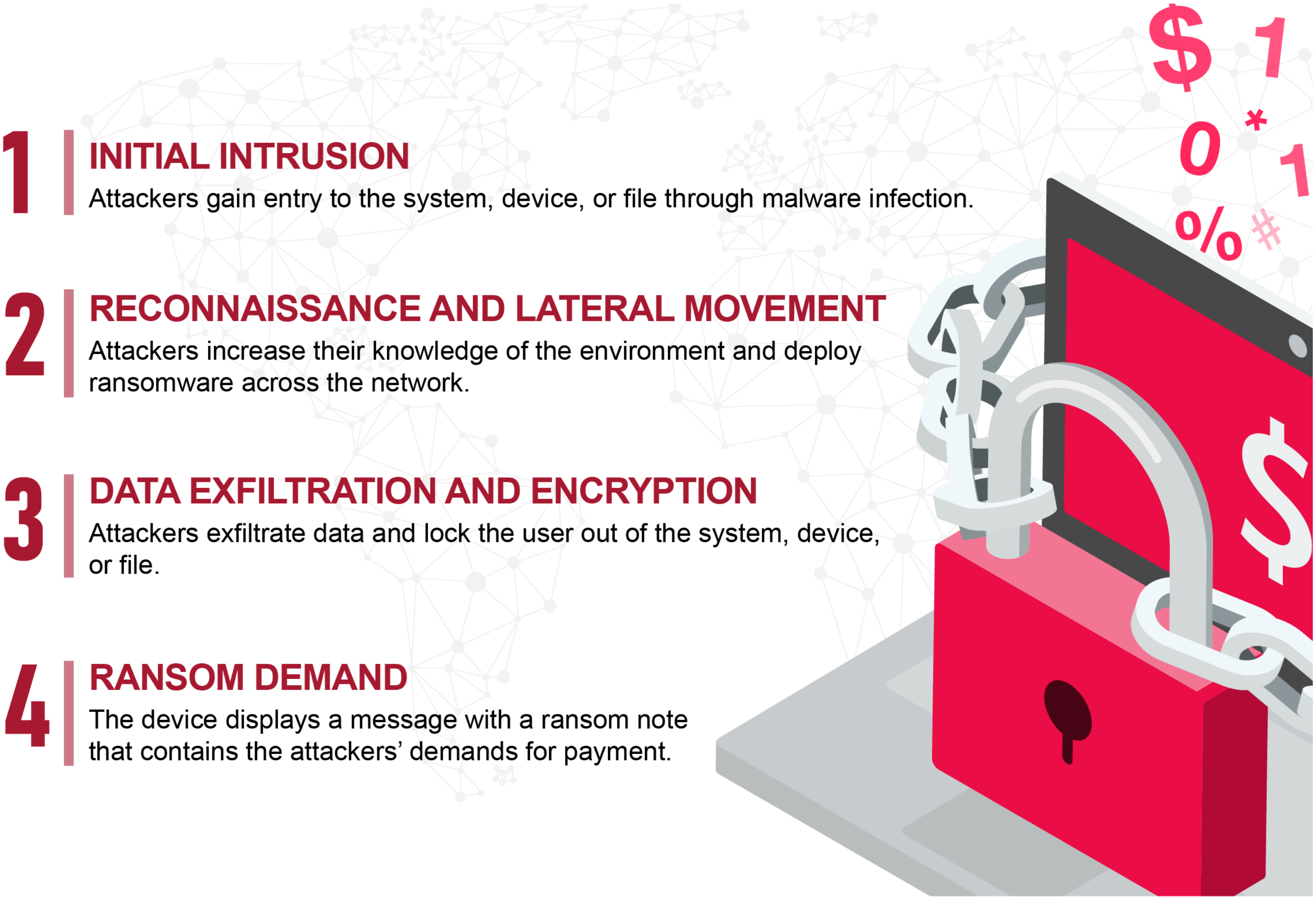
that compromised jail and courthouse computers. Also affected were data and systems related to election, assessment, financial, zoning, law enforcement, jail management, dispatch, and other data and systems, including a sheriff department's records management program.[17]

Ransomware Attacks Occur in Stages

A ransomware attack is not a single event. The attack occurs in a series of events or stages that include initial intrusion, reconnaissance and lateral movement, data exfiltration and encryption, and deployment. Figure 1 depicts four stages of a common ransomware attack.

[17] FBI, Cyber Division, *Private Industry Notification: Ransomware Attacks Straining Local US Governments and Public Services*, Private Industry Notification 20220330-001 (Mar. 30, 2022).

Figure 1: Four Stages of a Common Ransomware Attack



1 **INITIAL INTRUSION**
Attackers gain entry to the system, device, or file through malware infection.

2 **RECONNAISSANCE AND LATERAL MOVEMENT**
Attackers increase their knowledge of the environment and deploy ransomware across the network.

3 **DATA EXFILTRATION AND ENCRYPTION**
Attackers exfiltrate data and lock the user out of the system, device, or file.

4 **RANSOM DEMAND**
The device displays a message with a ransom note that contains the attackers' demands for payment.

Source: GAO analysis based on information from the Cybersecurity and Infrastructure Security Agency, Center for Internet Security, and Federal Bureau of Investigation; image: tomasknopp/stock.adobe.com. | GAO-22-104767

Initial intrusion. Malicious actors can launch a ransomware attack through a variety of common attack vectors. We have previously reported that malicious actors may make use of various techniques, tactics, and practices—or exploits—to adversely affect an organization's computers, software, or networks, or to intercept or steal valuable or sensitive information.[18] According to CISA, FBI, and MS-ISAC, initial intrusion can

[18] GAO, *Federal Information Security: Weaknesses Continue to Indicate Need for Effective Implementation of Policies and Practices*, GAO-17-549 (Washington, D.C.: Sept. 28, 2017).

occur through email phishing campaigns,[19] remote access technology,[20] third parties or service providers, existing malware infections, and software vulnerabilities. Once the malicious actors have compromised a device and obtained associated privileges to execute code, they can deploy ransomware.[21] For example:

- In July 2018, Laboratory Corporation of America or LabCorp, a medical testing company, experienced a ransomware attack. According to media reporting, the attack infected 7,000 computers and almost 2,000 servers using remote desktop.[22]
- In July 2021, Kaseya—a global IT management software company—experienced a cyberattack that resulted in a software supply chain compromise affecting almost 60 managed service providers who used its software to support services to small and medium sized businesses. The attack allowed malicious actors to compromise the provider's trusted relationships and launch ransomware attacks across almost 1,500 businesses with an initial ransom demand of $70 million to decrypt all affected systems.[23]

Reconnaissance and lateral movement. According to MS-ISAC, malicious actors perform reconnaissance to map out the network to ensure the most critical data are identified and targeted during the

[19] According to CISA, email phishing campaigns involve malware that can be downloaded onto a device through opening malicious files attached to the emails or by clicking on malicious links contained in the email or attachments. Malicious actors may also use legitimate, compromised email accounts to make phishing emails appear more authentic, potentially increasing their chances of getting a user to open an attached file or link.

[20] Remote access technology, such as remote desktop, allows individuals to control resources and data of a computer over the internet.

[21] According to MITRE, malicious actors may try to run code or manipulate system functions, parameters, and data in an unauthorized way. Execution consists of techniques that result in adversary-controlled code running on a local or remote system, device, or other asset. Execution may rely on unknowing end users or gaining elevated privileges.

[22] Steve Ragan, "Samsam Infected Thousands of LabCorp Systems via Brute Force RDP," CSO Online (CSO, July 19, 2018), https://www.csoonline.com/article/3291617/samsam-infected-thousands-of-labcorp-systems-via-brute-force-rdp.html.

[23] Office of the Director of National Intelligence, National Counterintelligence and Security Center, *Safeguarding Our Future: Kaseya VSA Supply Chain Ransomware Attack,* (Aug. 10, 2021), https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/Kaseya VSA Supply Chain Ransomware Attack.pdf.

ransomware encryption process.[24] Malicious actors typically seek to escalate their own privileges to an administrator level that provides greater access to a system or network by compromising the account. Once ransomware is on the system, malicious actors will look to move laterally across the network to spread the infection. Inadequate security controls allow the ransomware to spread across systems.

Data exfiltration and encryption. At this stage, malicious actors typically encrypt assets making them inaccessible to those who use them and/or exfiltrate data to force victims to make payments.[25] As previously mentioned, malicious actors may pressure victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary attempts to force payments. This includes publicly posting confidential data or selling the information in marketplaces on the dark web.

According to MS-ISAC, using data exfiltration as leverage over SLTT victims is especially impactful to organizations housing sensitive information, such as public health care entities and K-12 school districts. MS-ISAC also noted that malicious actors may even target former victims who paid ransoms, request additional payment, and threaten to publicly post the same data they allegedly deleted from the first attack after the ransom was paid.

Ransom demands. Ransom demands are typically in the form of cryptocurrency, or virtual currency,[26] such as Bitcoin. We previously reported that, according to federal agencies, virtual currency can be used in a variety of crimes, including drug and human trafficking, money laundering, cryptocurrency fraud, and as payment in ransomware attacks.[27]

According to MS-ISAC, the ransom amount will often vary based on the malicious actor's assessment of the victim's network and data as well as

[24] MS-ISAC, Center for Internet Security, "Security Primer – Ransomware," SP 2020-0002, (May 2020), https://www.cisecurity.org/insights/white-papers/security-primer-ransomware.

[25] According to NIST, exfiltration is the unauthorized transfer of information from a system.

[26] Virtual currencies are digital representations of value that are usually not government-issued legal tender and can include cryptocurrency, convertible virtual currency, and other industry labels such as digital assets and virtual assets.

[27] GAO, *Trafficking: Use of Online Marketplaces and Virtual Currencies in Drug and Human Trafficking,* GAO-22-105101 (Washington, D.C.: Feb. 14, 2022).

the ability and need to pay. According to MS-ISAC, the ransom note often expresses a sense of urgency, designed to motivate victims into paying the ransom quickly.

Ransom Payments Can Result in Follow-on Attacks and Civil Penalties, and Incentivize More Ransomware

CISA, FBI, Secret Service, and Treasury do not recommend paying ransom. According to CISA and MS-ISAC, doing so will not ensure that the data held hostage is decrypted or that systems or data will no longer be compromised.[28] Also, ransomware groups are known to share or sell victim information, including credentials, among each other to enable follow-on attacks. For example, CISA reported that the BlackMatter ransomware group, once shut down, transferred its existing victims to infrastructure owned by another group, known as Lockbit 2.0.

Ransomware payments may also lead to civil penalties from Treasury if the payments violate sanctions. In September 2021, Treasury issued an updated advisory to highlight the sanctions risks associated with ransomware payments in connection with malicious cyber-enabled activities. The advisory noted the proactive steps companies could take to mitigate such risks, including actions that Treasury would consider to be mitigating factors[29] in any related enforcement action.[30]

Treasury may also impose civil penalties for sanctions violations based on strict liability. This means that a person subject to U.S. jurisdiction may be held civilly liable even if such person did not know or have reason to know that it was engaging in a transaction that was prohibited under

[28] CISA and MS-ISAC, “Ransomware Guide,” (September 2020), https://www.cisa.gov/stopransomware/ransomware-guide.

[29] According to Treasury’s updated advisory, significant mitigating factors include voluntarily self-disclosing apparent violation of U.S. sanctions, completely reporting the ransomware attack as soon as possible to law enforcement or federal government agencies such as CISA, providing full and ongoing cooperation with law enforcement throughout the ransomware attack (e.g., providing all relevant information such as technical details, ransom payment demand, and ransom payment instructions as soon as possible), and reducing extortion risk by adopting and improving cybersecurity practices.

[30] Treasury, “Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments,” (Washington D.C.: Sept. 21, 2021). According to the updated advisory, Treasury would be more likely to resolve apparent sanctions violations involving ransomware attacks with a non-public response (i.e., No Action Letter or a Cautionary Letter) instead of a civil monetary penalty when the affected party took mitigating steps such as self-initiated complete reporting of the ransomware attack to law enforcement as soon as possible and providing ongoing cooperation.

sanctions laws and regulations administered by Treasury.[31] Treasury emphasized that ransomware payments made to sanctioned persons or to sanctioned jurisdictions could be used to fund activities adverse to the national security and foreign policy objectives of the United States and incentivize additional attacks.

In addition to potentially resulting in follow-on attacks and civil penalties, making ransomware payments can also encourage criminals' continued use of ransomware. In February 2022, CISA released an advisory in which the cybersecurity authorities in the United States, Australia, and the United Kingdom noted that every time a ransom is paid, it confirms the viability and financial attractiveness of the ransomware criminal business model.[32]

The Ransomware Threat in the U.S. Is Pervasive and Costly

Similar to other types of criminal activity, the number of reported ransomware events cannot be precisely identified due to the voluntary nature of the reporting and potential reluctance to report being a victim. Given the variety of reporting mechanisms, there is not a single source for a total number of ransomware events reported to the federal government and the reporting to federal agencies likely does not capture the full number and financial impact of such incidents.[33] Nonetheless, several federal and private sector sources indicate that ransomware threats have

[31] According to Treasury, its Office of Foreign Assets Control's sanctions prohibit U.S. persons from engaging in unauthorized transactions, directly or indirectly, with comprehensively sanctioned jurisdictions (e.g., Cuba, certain covered regions of Ukraine, Iran, North Korea, and Syria) and sanctioned persons, including individuals or entities on the Office of Foreign Assets Control's Specially Designated Nationals and Blocked Persons List (SDN List). U.S. persons, wherever located, are also generally prohibited from facilitating actions of non-U.S. persons that could not be directly performed by U.S. persons due to U.S. sanctions regulations.

[32] CISA, "2021 Trends Show Increased Globalized Threat of Ransomware," Alert (AA22-040A) (Feb. 9, 2022), accessed Feb. 9, 2022, https://www.cisa.gov/uscert/ncas/alerts/aa22-040a.

[33] The *Cyber Incident Reporting for Critical Infrastructure Act of 2022*, enacted on March 15, 2022, division Y of the Consolidated Appropriations Act, 2022, Pub. L. No. 117-103, div. Y, 136 Stat. 49, 1038 (2022), will require covered entities across critical infrastructure sectors to report "covered cyber incidents" to CISA within 72 hours of reasonably determining a "covered cyber incident" occurred and ransom payments within 24 hours of payment. 6 U.S.C. § 681b(a). CISA has not yet issued rules for such reporting. It has 24 months from the date the act was signed into law to issue the proposed rule, and 18 months from the publication of the proposed rule to publish a final rule. 6 U.S.C. § 681b(b).

escalated over time, and are becoming more sophisticated, pervasive, and costly.

Federal agencies have reported on ransomware trends over time to monitor the threat to organizations. While it is clear that ransomware attacks are occurring at an alarming rate, the data on ransomware attacks are likely underreported because federal agencies rely on voluntary information from SLTTs. For example, the MS-ISAC, which tracks and responds to SLTT incidents on behalf of CISA, stated that its research found more than 2,800 ransomware incidents against SLTTs from January 2017 through March 2021. However, SLTTs only reported 741 incidents to the MS-ISAC from October 2017 through February 2022, less than one-third of the incidents found through MS-ISAC's own research.[34]

Further, the FBI's Internet Crime Complaint Center (IC3)—which obtains and analyzes reports of internet-related crimes from victims such as business and the general public reported almost 2,500 ransomware complaints in 2020[35] and more than 3,700 in 2021.[36] These reports included 649 incidents that affected 14 of the 16 critical infrastructure sectors. Health care/public health and government facilities were among the top five infrastructure sectors victimized by ransomware.

Verizon also reported in its 2020 annual data breach report that ransomware continues to be a top incident type and it represents a disproportionate percentage of malware attacks affecting the public administration sector relative to other types of malware compromises. Specifically, ransomware accounts for 60 percent of malware compromises affecting the public administration sector compared to 27

[34] According to CISA, in some instances, the MS-ISAC became aware of the ransomware attack months after the incident occurred. In these cases, the incidents were logged and assistance was made available to the victim. In addition, SLTTs may not always request federal assistance or report to federal agencies.

[35] FBI Internet Crime Complaint Center, "Internet Crime Report 2020," accessed Apr. 13, 2021, https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf. FBI's IC3 statistics did not identify the number of SLTTs affected and may include individuals and private sector entities. FBI also noted in its report that the reported losses were artificially low and its data did not include direct reports to field offices.

[36] FBI Internet Crime Complaint Center, "Internet Crime Report 2021," https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf.

percent of malware compromises across all sectors.[37] In its 2022 report, Verizon reported that ransomware incidents increased 13 percent since 2021—more than in the last 5 years combined.[38] In addition, cybersecurity vendor Emsisoft identified that 2,323 ransomware attacks occurred in 2021 on local governments, schools, and health care providers and more than one-third of ransomware attacks on local governments resulted in data breaches with extremely sensitive information subsequently released online.[39]

With the increasing number of attacks, ransomware costs have also been steadily growing. According to CISA, the monetary value of ransom demands has increased over time, with some demands exceeding $1 million today. In addition, Treasury reported that in 2020, ransomware payments reached over $400 million, more than four times the level in 2019.[40] Additionally, Treasury's Financial Crimes Enforcement Network reported that the total value of suspicious activity[41] during the first 6 months of 2021 was $590 million, which exceeds the value reported for the entirety of 2020 ($416 million).[42]

Moreover, the above costs only address the financial impacts from payments. Ransomware attacks have other costs associated with recovering and restoring systems such as staff downtime while systems are inaccessible and the need to hire additional staff to restore data from backups or rebuild networks. According to cybersecurity research by

[37] Verizon, *2020 Data Breach Investigations Report*. https://www.verizon.com/business/resources/reports/dbir/2020/introduction/.

[38] Verizon, *2022 Data Breach Investigations Report*. https://www.verizon.com/business/resources/reports/dbir/.

[39] Emsisoft, "The State of Ransomware in the US: Report and Statistics 2021." Web Blog, Jan. 18, 2022. https://blog.emsisoft.com/en/40813/the-state-of-ransomware-in-the-us-report-and-statistics-2021/.

[40] Treasury, "Treasury Takes Robust Actions to Counter Ransomware," (Sept. 21, 2021), accessed Sept. 22, 2021, https://home.treasury.gov/news/press-releases/jy0364.

[41] Suspicious activity reports capture known or suspected violation of federal law or a suspicious transaction related to a money laundering activity or a violation of the Bank Secrecy Act, including ransomware.

[42] Treasury, Financial Crimes Enforcement Network, "Financial Trend Analysis: Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021," Retrieved from https://www.fincen.gov/news/news-releases/fincen-issues-report-ransomware-trends-bank-secrecy-act-data.

Sophos, these costs can be up to 10 times greater than the actual ransomware payment. There are also intangible costs, such as the health and safety implications when ransomware renders a hospital's IT systems unusable.

Over the last 3 years, there have been several public reports on federal actions taken against malicious actors and notable ransomware attacks on critical infrastructure, educational institutions, and local government operations.[43] For example:

- In June 2021, the White House and U.S. Department of Agriculture announced that a meat processing company had been targeted with ransomware that affected the company's operations.[44] News services reported that the company paid $11 million in ransom.
- In May 2021, Colonial Pipeline Company announced that it was the victim of a ransomware attack that led to temporary disruption in the delivery of gasoline and other petroleum products across much of the southeast U.S., and paid over $4 million in ransom. According to DOJ, it seized over $2.3 million allegedly paid to the ransomware group that launched the ransomware attack.[45]
- In February 2021, DOJ announced that three North Korean individuals were indicted for, among other things, the creation of the destructive WannaCry ransomware, as well as the extortion and attempted extortion of victim companies from 2017 through 2020.[46] The WannaCry campaign, which was discovered in May 2017, remotely

[43] GAO, "Ransomware—Holding IT Systems and Data Hostage." Web Blog. WatchBlog, June 30, 2021. https://www.gao.gov/blog/ransomware-holding-it-systems-and-data-hostage.

[44] Department of Agriculture, "Statement from the U.S. Department of Agriculture on JBS USA Ransomware Attack," (June 1, 2021), accessed Aug. 18, 2022, https://www.usda.gov/media/press-releases/2021/06/01/statement-us-department-agriculture-jbs-usa-ransomware-attack.

[45] Department of Justice, "Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside," (June 7, 2021), accessed Dec. 28, 2021, https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside.

[46] Department of Justice, "Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe," (Feb. 17, 2021), accessed Aug. 18, 2022, https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and.

compromised systems and encrypted files, affecting hospitals, schools, businesses, and numerous organizations. It led to tens of thousands of infections in over 150 countries.

- In December 2020, federal law enforcement received numerous reports of ransomware attacks against K-12 educational institutions. In these attacks, malicious cyber actors targeted school computer systems, slowing access, and—in some instances—rendering the systems inaccessible for basic functions, including distance learning. We also recently reported on the increasing number of ransomware incidents and cybersecurity threats to K-12 schools.[47]
- In October 2020, DOJ announced that six Russian individuals were indicted for a series of computer attacks including NotPetya ransomware, which caused nearly $1 billion in losses to the three known victims identified in the indictment.[48] NotPetya, which was discovered in June 2017, was a form of malware that exploited existing vulnerabilities in computer software or networks to encrypt files and allowed attackers to gain privileged rights and encrypt essential files making the infected Windows computers unusable. It infected organizations in several sectors, including finance, transportation, energy, commercial facilities, and health care.
- In July 2019, CISA, MS-ISAC, National Governors Association, and National Association of State Chief Information Officers issued a joint statement due to ransomware attacks targeting systems across the country, including a string of attacks affecting state and local government partners.[49]
- In May 2019, the Mayor of Baltimore reported that the city was the victim of a ransomware attack. As a result, city employees were not able to access their emails and the attack delayed real estate sales and water billing for months.

[47] GAO-22-105024.

[48] Department of Justice, “Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace,” (Oct. 19, 2020), accessed July 6, 2022, https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and.

[49] CISA, MS-ISAC, National Association of State Chief Information Officers, National Governors Association, “CISA, MS-ISAC, NGA & NASCIO Recommend Immediate Action to Safeguard Against Ransomware Attacks,” (Washington D.C.: July 29, 2019).

Federal Guidelines and Key Practices Support Interagency Coordination of Cybersecurity Response Efforts

In 2016, the administration issued Presidential Policy Directive-41 (PPD-41), *United States Cyber Incident Coordination*, which set forth principles governing the federal government's response to any cyber incident, whether involving government or private sector entities, to achieve unity of effort and coordination.[50] PPD-41 is intended to provide a framework or guiding principles for supporting policies, procedures, and mechanisms established by relevant federal agencies. Further, an annex to PPD-41 provided further details concerning the federal government's coordination on cyber incidents deemed to be significant and prescribed additional principles for agencies to implement.[51] We have previously reported on federal use of PPD-41 procedures to test coordinated cyber incident response efforts.[52] Among other things, the directive called for federal agencies to respond to cyber incidents by implementing four coordination principles that are applicable to federal agencies when assisting SLTTs with ransomware incidents:

- **Lead agency roles:** implementing the roles of designated lead federal agencies for asset response[53] and threat response[54] activities.
- **Agency coordination**: coordinating to provide unity of effort on threat response and asset response activities.
- **Field-level coordination:** coordinating field-level activities within their respective lines of effort with each other and the affected entity.

[50] A cyber incident is an event occurring on or conducted through a computer network that actually or imminently jeopardizes the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon. A cyber incident may include a vulnerability in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

[51] A significant cyber incident is a cyber incident that is (or group of related cyber incidents that together are) likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.

[52] GAO, *Cybersecurity: Internet Architecture Is Considered Resilient, but Federal Agencies Continue to Address Risks,* GAO-22-104560 (Washington, D.C.: Mar. 3, 2022).

[53] Asset response activities include furnishing technical assistance to affected entities to protect their assets, mitigate vulnerabilities, and reduce impacts of cyber incidents; facilitating information sharing and operational coordination with threat response; and providing guidance on how best to utilize federal resources.

[54] Threat response activities include conducting appropriate law enforcement and national security investigative activity at the affected entity's site, collecting evidence, and gathering intelligence.

- **Unified public communications:** establishing unified public communications by maintaining fact sheets that outline how organizations can contact federal agencies about a cyber incident.[55]

Additionally, we have previously identified seven key practices that can enhance and sustain interagency coordination.[56] These practices are consistent with the guiding principles of PPD-41[57] and provide actions for agency officials to consider when working collaboratively through a variety of different mechanisms, such as task forces or interagency working groups throughout government.[58] Such actions can help to ensure a unified, coordinated federal effort when providing prevention and response assistance for ransomware within the SLTT community. The seven key practices are:

- **Defining outcomes and monitoring accountability** addresses whether short- and long-term outcomes have been clearly defined,

[55] PPD-41 identifies agency coordination and field-level coordination as principles for responding to "significant" cyber incidents. Each ransomware incident that occurs on SLTTs may not rise to the threshold of a "significant" cyber incident as defined by PPD-41. However, we applied these principles to our analysis because the three federal agencies that interact with SLTTs on reported ransomware-related incidents—CISA, FBI, and Secret Service—stated that they coordinate with each other at an agency-level and through field-level coordination consistent with PPD-41.

[56] GAO, *Managing for Results: Key Considerations for Implementing Interagency Collaborative Mechanisms,* GAO-12-1022 (Washington, D.C.: Sept. 27, 2012).

[57] Several of the key collaboration practices also relate to the four cyber incident coordination principles identified in PPD-41. For example, the directive calls for federal agencies to develop policies and procedures that address how they coordinate at the agency level and in the field. This relates to all seven collaboration practices to some degree as each of the practices address specific aspects of agency- and field-level coordination. In addition, the directive identifies DHS and DOJ as lead federal agencies for asset and threat response, respectively. It also notes that DHS and DOJ are to establish unified public communications through an updated fact sheet outlining how private individuals and organizations can contact relevant federal agencies about a cyber incident. These cyber incident coordination practices are related to the key collaboration practices associated with identifying and sustaining leadership, and clarifying roles and responsibilities.

[58] Federal agencies can use a variety of mechanisms to implement interagency collaborative efforts, such as the President appointing a coordinator, agencies co-locating within one facility, or establishing interagency task forces. Regardless of the mechanism used, participating agencies should reach agreement on a collaborative mechanism that implements our seven key practices. For example, jointly defined goals, outcomes, and a mechanism for tracking and monitoring progress ensures that participating agencies work towards shared goals and can evaluate the effectiveness of collaborative efforts on a continual basis (GAO-12-1022).

and the extent tracking and monitoring of progress in achieving outcomes has been performed.

- **Bridging organizational cultures** includes identifying the missions and cultures of the participating organizations in the collaborative groups and developing ways to operate across agency boundaries.
- **Identifying and sustaining leadership** involves designating agency leads or individuals who will lead the collaborative efforts.
- **Clarifying roles and responsibilities** addresses whether the participating agencies have clarified roles and responsibilities and processes are in place for making decisions.
- **Including participants** ensures that all relevant participants are involved in the collaborative efforts and have the ability to regularly attend activities of the collaborative mechanism.
- **Identifying and leveraging resources** involves leveraging relevant staff and IT resources to support the operations of the collaborative efforts.
- **Developing and updating written guidance and agreements** includes documenting the participating agencies' agreement regarding how they will collaborate, and determining ways to continually update and monitor these agreements.

Federal Agencies Provide Ransomware Assistance to State, Local, Tribal, and Territorial Governments

CISA, FBI, and Secret Service are the primary federal agencies that provide direct ransomware assistance to SLTTs. These agencies interact with SLTTs to provide education and awareness, technical information sharing and analysis, cybersecurity review and assessment, and incident response. Other federal agencies, such as FEMA, National Guard Bureau, NIST, and Treasury support SLTTs by providing indirect ransomware assistance and generally do not interact directly with SLTTs. These agencies provide indirect assistance that support SLTTs and combat ransomware through activities such as administering cybersecurity grants, issuing policy or technical guidance, and imposing sanctions as a result of ransomware.

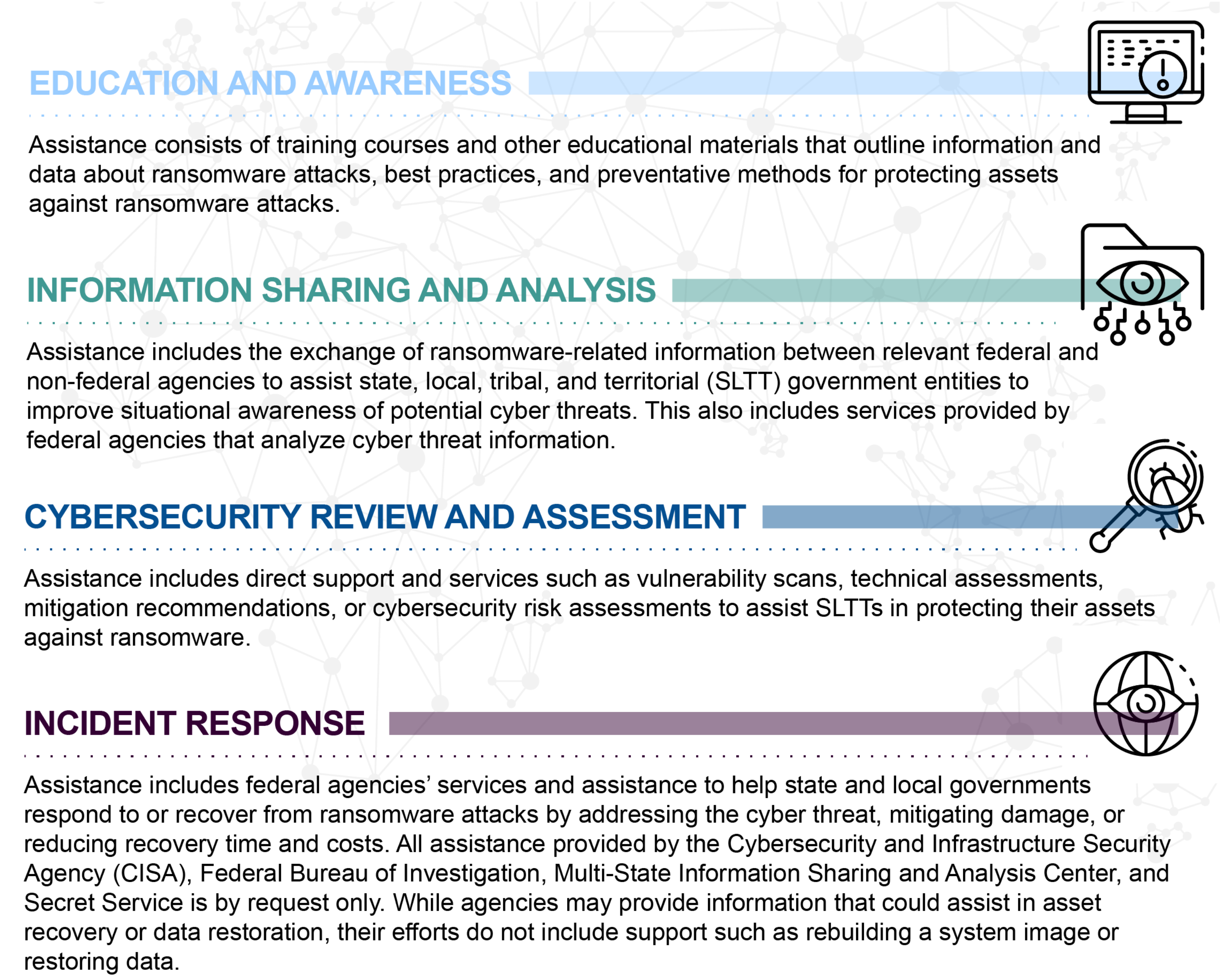
CISA, FBI, and Secret Service Provide Ransomware Assistance Directly to State and Local Governments

CISA, FBI, and Secret Service provide direct assistance[59] aimed at preventing ransomware attacks on SLTTs through education and awareness, technical information sharing and analysis, and cybersecurity review and assessment.[60] In addition, these agencies provide direct assistance upon request for responding to ransomware incidents by conducting technical analysis and conducting investigations on threat actors. Figure 2 identifies and defines each type of assistance available to SLTTs, and is followed by a discussion on the federal agencies who offer such assistance.

[59] Direct assistance involves interaction between a SLTT organization and federal agency in order to request and provide services and support for ransomware prevention and response.

[60] Agencies may proactively share information with SLTTs for prevention and mitigation purposes. Additionally, agencies provide certain services by request such as technical analyses and assessments.

Figure 2: Types of Ransomware Assistance Available to State, Local, Tribal, and Territorial Organizations



EDUCATION AND AWARENESS

Assistance consists of training courses and other educational materials that outline information and data about ransomware attacks, best practices, and preventative methods for protecting assets against ransomware attacks.

INFORMATION SHARING AND ANALYSIS

Assistance includes the exchange of ransomware-related information between relevant federal and non-federal agencies to assist state, local, tribal, and territorial (SLTT) government entities to improve situational awareness of potential cyber threats. This also includes services provided by federal agencies that analyze cyber threat information.

CYBERSECURITY REVIEW AND ASSESSMENT

Assistance includes direct support and services such as vulnerability scans, technical assessments, mitigation recommendations, or cybersecurity risk assessments to assist SLTTs in protecting their assets against ransomware.

INCIDENT RESPONSE

Assistance includes federal agencies' services and assistance to help state and local governments respond to or recover from ransomware attacks by addressing the cyber threat, mitigating damage, or reducing recovery time and costs. All assistance provided by the Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation, Multi-State Information Sharing and Analysis Center, and Secret Service is by request only. While agencies may provide information that could assist in asset recovery or data restoration, their efforts do not include support such as rebuilding a system image or restoring data.

Source: GAO analysis based on information from federal agencies; image: tomasknopp/stock.adobe.com, ylivdesign/stock.adobe.com. | GAO-22-104767

Education and Awareness

CISA provides education and awareness assistance to state and local governments through its publication of guidance and alerts, as well as exercises and campaigns. For example, CISA officials stated that in fiscal years 2021 and 2022, the agency conducted 50 ransomware-related tabletop exercises for SLTT governments with about 3,900 participants that simulated scenarios to enhance planning, collaboration, and information sharing. Additionally, in January 2021, CISA launched a 6-month Reduce the Risk of Ransomware campaign to raise awareness about the importance of combating ransomware as part of an organization's cybersecurity and data protection best practices. As part of its campaign, CISA used its social media platforms to reiterate key behaviors or actions to help SLTTs combat ransomware and hosted a ransomware seminar on prevention for more than 3,100 attendees.

Related to this effort, CISA launched the first iteration of a ransomware website now known as www.stopransomware.gov, which received more than 115,000 views during the campaign. In collaboration with FBI, Secret Service, and other federal partners, the website provides a central location for ransomware protection, detection, and response guidance to assist ransomware victims. In addition, the website provides central access to ransomware-related resources such as alerts, advisories, and reports from multiple federal agencies and partners.

For example, CISA, in partnership with MS-ISAC,[61] published the *CISA and MS-ISAC Ransomware Guide* that provides recommendations and best practices for IT professionals and others involved in the development of cyber incident response policies and procedures.[62] The two-part guide includes information on initial infection vectors, such as software vulnerabilities and misconfigurations, as well as phishing for ransomware.[63] It also includes associated recommendations for network defense.

Additionally, the **FBI and Secret Service** provide education and awareness on ransomware through guidance, reports, and brochures

[61] The Center for Internet Security operates the MS-ISAC under a cooperative agreement with DHS. MS-ISAC membership is open to all state, local, tribal, and territorial government entities and includes over 2,500 MS-ISAC member organizations, including 79 fusion centers, across public sectors such as government, education, utilities, and transportation. As of February 2022, there were 12,797 MS-ISAC members (including all 50 states). MS-ISAC provides a number of information sharing resources and cybersecurity assessments to SLTTs that are supported by funding from CISA through a DHS cooperative agreement.

[62] CISA and MS-ISAC, "Ransomware Guide," Ransomware Guide (September 2020), https://www.cisa.gov/stopransomware/ransomware-guide.

[63] According to NIST, phishing is a technique to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a website, in which the perpetrator masquerades as a legitimate business or reputable person.

disseminated using agency websites and through the FBI's Cyber Task Forces and Secret Service's Cyber Fraud Task Forces that are located at field offices throughout the country. These agencies' guidance provide detailed assessments of ransomware characteristics and how to prepare, prevent, and respond to ransomware attacks.

Specifically, the FBI developed a brochure that explains how ransomware can infect a network through both human and technical weaknesses in an organization.[64] The brochure provides key areas to focus on in regards to ransomware, such as prevention, business continuity, and other related considerations. For example, it describes the necessity for training and awareness against the threat, technical controls to implement, such as access control methods, and the importance of securing data backups to maintain business continuity.

Similarly, Secret Service's guidance includes a list of ransomware characteristics and preventative measures.[65] For example, the guide recommends application whitelisting, which is a defined list of applications and their components authorized for use within an organization. According to the guide, this method reduces the risk of ransomware execution and unauthorized software, which is a common attack vector.

Secret Service and the FBI also held events to further educate SLTTs and enhance readiness for cyber risks such as ransomware. For example, FBI officials noted that the agency held a webinar in 2020 with over 5,000 participants from the SLTT community to train and educate individuals on cybercrime with a focus on ransomware. Secret Service officials also noted that additional training is available to SLTTs of the law enforcement community through the National Computer Forensics Institute. The training focuses on recovery from a data breach and best practices for preventing ransomware attacks.

Information Sharing and Analysis

CISA and the MS-ISAC collect and analyze security and ransomware-related information—such as threat indicators, incident alerts, and vulnerability data—and share this information by issuing alerts and advisories in a variety of ways for situational awareness. Specifically,

[64] FBI, Cyber Division, *Ransomware*, https://www.ic3.gov/Content/PDF/Ransomware_Trifold_e-version.pdf.

[65] United States Secret Service, Cybercrime Investigations, "*Preparing for a Cyber Incident: A Guide to Ransomware,"* https://www.secretservice.gov/investigation/Preparing-for-a-Cyber-Incident.

CISA shares information through its Homeland Security Information Network and Automated Indicator Sharing platform. In addition, CISA, in coordination with the MS-ISAC, shares cyber threat information for network defense purposes with the MS-ISAC's membership of almost 13,600 SLTTs, as of May 2022.[66] Center for Internet Security officials noted that they also receive important cyber threat information from SLTT members that is used to inform its analysis and information sharing efforts.

CISA has issued 33 official alerts and statements on the www.stopransomware.gov website regarding ransomware activity. Seventeen of those alerts were in partnership with the FBI, Department of Health and Human Services, MS-ISAC, National Security Agency, Secret Service, and international governments, as of June 2022. For example:

- In February 2020, CISA released an alert to provide information and technical details about a ransomware attack that targeted pipeline operations, affecting network control and communications. The advisory includes guidance on applying appropriate mitigations for asset owners and operators across all critical infrastructure sectors.
- In September 2021, CISA, FBI, and the National Security Agency published a joint advisory on Conti ransomware with technical details and recommended mitigations. The advisory noted that CISA and the FBI had observed the increased use of Conti ransomware in more than 400 attacks on U.S. and international organizations to steal files, encrypt servers and workstations, and demand a ransom payment.
- In October 2021, CISA, FBI, and the National Security Agency issued a joint alert to provide information on BlackMatter ransomware, which has targeted multiple U.S. critical infrastructure sectors, including two U.S. Food and Agriculture Sector organizations. This advisory provided information on cyber actor tactics, techniques, and procedures obtained from a sample of BlackMatter ransomware analyzed in a sandbox environment as well from trusted third party reporting.[67]

[66] CISA's and MS-ISAC's cyber threat information is based on data from incidents where they provided technical assistance, the indicators of compromise of those incidents, and additional information and experiences shared by SLTTs, federal, industry, and international partners.

[67] A sandbox environment is a system that allows an untrusted application to run in a highly controlled environment where the application's permissions are restricted to an essential set of computer permissions.

CISA also analyzes suspected malicious files by using its Advanced Malware Analysis Center. In addition, the MS-ISAC uses its Malicious Code Analysis Platform. These capabilities provide, among other things, analysis of malicious code when a stakeholder or member submits samples online. The stakeholder will then receive a technical analysis outlining the results and recommended actions.

In partnership with CISA, the MS-ISAC offers two enhanced network defense services. Specifically, it offers an intrusion detection system (referred to as Albert sensors) that can recognize and alert on potentially malicious traffic occurring on a network. The sensors detect potentially malicious threats through MS-ISAC research, commercial detection signatures, and indicators of compromise derived from past malicious activity.[68] According to the MS-ISAC, its sensors analyze 1 trillion logs per month. The MS-ISAC also reported that its sensors detected 300 ransomware infections, potentially saving SLTTs more than $22 million in 2018 and 2019. According to the MS-ISAC, as of June 2022, it deployed 896 total Albert sensors for SLTTs.[69]

The MS-ISAC also provides a malicious domain blocking and reporting service at no cost to SLTTs. This service blocks known malicious links in phishing emails or web addresses used as command and control by adversaries to download or control malware such as ransomware. According to the Center for Internet Security, by July 2020, the MS-ISAC's service had blocked more than 1.5 billion requests to known bad web domains preventing potential malware or ransomware infections that could have affected about 4,500 SLTTs.

Additionally, the **FBI and Secret Service** collect evidence to investigate and analyze ransomware data, and help prevent repeat attacks through sharing intelligence. Specifically, the FBI shares information it receives on a specific threat with SLTTs, federal agencies, and private sector partners by releasing private industry notifications, issuing flash alerts on technical

[68] Information from past malicious activity includes information observed by the MS-ISAC or as shared by CISA and other partners.

[69] According to the Center for Internet Security, the federal government covered the cost of the sensors for 204 SLTTs through its cooperative agreement funding. The Center for Internet Security noted that given the value provided by its intrusion detection sensors, SLTTs purchased 692 additional sensors.

indicators of compromise, and exchanging information from the InfraGard platform.[70] For example:

- In November 2021, the FBI issued a private industry notification stating that ransomware actors were very likely to use significant financial events, such as mergers and acquisitions, to target and leverage victim companies for ransomware infections.[71] Prior to an attack, ransomware actors research publicly available information, such as a victim's stock valuation, as well as material nonpublic information. If victims do not pay a ransom quickly, ransomware actors may threaten to disclose this information publicly, causing potential investor backlash. This notification included an assessment of the threat and technical recommendations to safeguard systems.
- In October 2021, the FBI released a flash alert on the tactics, techniques, and indicators of compromise associated with Hello Kitty/FiveHands ransomware.[72] It also included technical recommendations to safeguard systems and general response procedures. The alerts are to inform and equip private industry and SLTTs with threat information needed to make appropriate cyber decisions.

In addition, the FBI's IC3 is a mechanism to receive online complaints from the public, alert the public of cyber threats, and share data with other law enforcement partners. It is also one of the FBI's primary mechanisms used to receive reports from victims of cybercrime.[73] IC3 collects and

[70] InfraGard is an information sharing platform in partnership between FBI and private sector members who promote the protection of U.S. critical infrastructure. SLTTs can participate to receive information sharing, networking, and workshops on emerging technologies and threats, including ransomware. Membership includes business executives, entrepreneurs, lawyers, security personnel, military and government officials, IT professionals, academia and state and local law enforcement. Among other qualifications, members must be affiliated with any one of the 16 critical infrastructure sectors.

[71] FBI, Cyber Division, *Ransomware Actors Use Significant Financial Events and Stock Valuation to Facilitate Targeting and Extortion of Victims*, Private Industry Notification (20211101-001) (Nov. 1, 2021), https://www.cisa.gov/stopransomware/official-alerts-statements-fbi.

[72] FBI, Cyber Division, *Tactics, Techniques, and Indicators of Compromise Associated with Hello Kitty/FiveHands Ransomware*, FLASH (CU-000154-MW) (Oct. 28, 2021), https://www.cisa.gov/stopransomware/official-alerts-statements-fbi.

[73] According to the FBI, it may receive cyber incident reports from victims through several mechanisms, such as standing relationships between a field office and a key entity within that office's territory, call-ins to a field office or FBI's national intake center, and IC3.gov.

analyzes report data to identify and track emerging cyber threats. IC3 also provides alerts on its public website that provide ransomware-related and cyberattack information.

Further, Secret Service collaborates with the FBI and CISA to issue joint alerts and advisories on ransomware variants. For example, in February 2022, all three agencies jointly issued an advisory for BlackByte ransomware, which included indicators of compromise[74] and mitigations.

Cybersecurity Review and Assessment

CISA, in partnership with the MS-ISAC, is the primary federal agency that provides cybersecurity review and assessment to SLTTs. The FBI and Secret Service primarily serve in an information sharing and investigative role. Therefore, they do not provide cybersecurity reviews and assessments of SLTTs' resilience to ransomware attacks.

CISA and the MS-ISAC provide direct assistance to SLTTs, when requested, through cybersecurity reviews and assessments intended to help with hardening networks and enhancing cyber threat awareness. The review and assessment services are available at no cost to SLTTs.[75] For example, CISA provides a suite of scanning and testing services to help SLTTs assess, identify, and reduce their exposure to threats, including ransomware. This suite includes:

- Vulnerability scanning: Formerly known as cyber hygiene scanning, this assessment scans information systems for known weaknesses. Once entities are enrolled, scans continue on a weekly basis.
- Web application scanning: These scans evaluate publicly-accessible websites for potential bugs and weak configurations to provide recommendations for mitigating web application security risks.
- Phishing campaign assessment: The phishing assessment is a 6-week engagement offered to SLTTs to evaluate an organization's susceptibility and reaction to phishing emails.

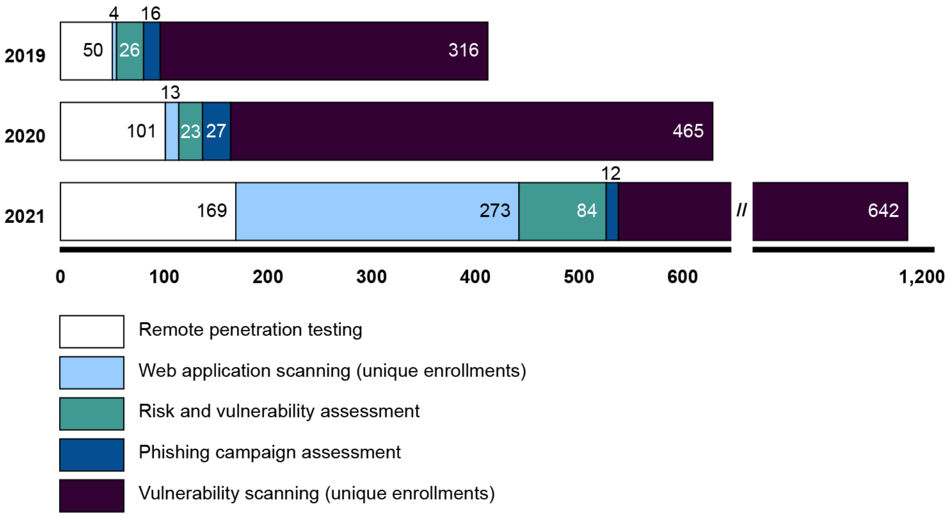
[74] Indicators of compromise refer to identification of forensic evidence from an organization's systems at the host or network level. Indicators of compromise are comprised of threat indicators, signatures, and techniques that IT professionals can use to identify unusual or irregular network activity.

[75] According to CISA, its total budget for funding MS-ISAC and Elections Infrastructure Information Sharing and Analysis Center services in fiscal year 2020 was $23,294,000 and $26,344,000 in fiscal year 2021. This budget does not cover the entirety of SLTT support as other CISA services and programs are available to all 16 critical infrastructure sectors and SLTTs, at no cost.

- Remote penetration testing: These tests simulate the tactics and techniques of real-world adversaries to identify and validate exploitable pathways. This service tests perimeter defenses, the security of externally-available applications, and the potential for exploitation of open source information.

Figure 3 depicts the growth in the number of SLTTs enrolled in CISA's suite of scanning and testing services in recent years.

Figure 3: Number of Enrollments in Cybersecurity and Infrastructure Security Agency's (CISA) Scanning and Testing Services



Source: GAO analysis of data reported by CISA. | GAO-22-104767

Note: The figure does not depict total numbers of assessments provided over a period of time, but rather, depending on the assessment, depicts either new, unique enrollments or new assessments provided in each associated fiscal year.

CISA also provides, or funds through the MS-ISAC, additional products and services that it considers effective in helping SLTTs protect their systems and build resilience against ransomware. For example, CISA can provide assessments, such as cyber infrastructure surveys, which evaluate the effectiveness of organizational security controls, preparedness, and overall resilience. Additionally, CISA's external dependencies management assessments help SLTTs manage the risk introduced by third-party managed service providers. If compromised, such managed service providers lead malicious actors to state and local governments through managed infrastructure or compromised service accounts. Table 1 identifies seven products and services that CISA considered effective in addressing ransomware threats for state and local governments.

Table 1: Products and Services That the Cybersecurity and Infrastructure Security Agency (CISA) Highlighted as Effective in Addressing State and Local Government Ransomware Threats

Products and services	Organization that provided product or service	Time frame of product or service provided[a]	Number of times state, local, tribal, or territorial governments received product or service
Cyber infrastructure survey This service uses a voluntary survey that evaluates the effectiveness of organizational security controls, cybersecurity preparedness, and overall resilience.	CISA	October 2018 – February 2022	164
Cyber resilience review This service uses a voluntary, interview-based assessment to evaluate an organization's operational resilience and cybersecurity practices.	CISA	October 2018 – February 2022	189
Endpoint detection and response This service is funded by CISA and helps state and local government entities involved in managing elections maintain awareness of and isolate malicious activity that may be impacting workstations, servers, and other network endpoints, including malware and ransomware.	Multi-state Information Sharing and Analysis Center (MS-ISAC)	July 2019 – May 2022	319
External dependencies management assessments This service uses an interview-based assessment to evaluate an organization's management of their dependencies. The assessment focuses on the relationship between an organization's services and assets and evaluates how well the organization manages risk that might occur.	CISA	October 2018 – February 2022	97
Malicious domain blocking and reporting This service is funded by CISA and blocks known malicious links in phishing emails or web addresses used as command and control by adversaries to download or control malware or ransomware.	MS-ISAC	July 2019 – May 2022	4,451
Nationwide cybersecurity review This service is funded by CISA and includes an annual, self-assessment survey that is intended to help state and local entities assess the effectiveness of and identify gaps in their cybersecurity programs and initiatives. The review is aligned with the National Institution of Standards and Technology's Cybersecurity Framework to help entities identify and prioritize actions for reducing cybersecurity risks. The review is offered once per year.	MS-ISAC	October 2021- Feburary 2022	3,267
Ransomware readiness assessment This service is a self-assessment based on a tiered set of practices to help organizations better assess how well they are equipped to defend and recover from a ransomware incident. The metric refers to the total number of downloads as of March 31, 2022, for all different versions of the assessments released.	CISA	June 2021 – March 2022	20,409

Source: GAO analysis of data reported by CISA and MS-ISAC. | GAO-22-104767

[a]The depicted timeframes and related statistics represent a snapshot in time and are based on when the information was requested and provided. These products and services are provided to SLTT governments on an ongoing basis.

To manage partnerships and offer services, CISA employs personnel with cyber and physical security expertise in its 10 regional offices throughout the country who conduct outreach to SLTTs on services and assessments. According to CISA, as of February 2022, these experts included 57 cybersecurity advisors. A single advisor may be responsible for performing and coordinating assessments for an entire state or region and across multiple cybersecurity-related issues and for multiple sectors of critical infrastructure. CISA officials stated that, although its advisors promote the agency's services and conduct survey-based risk management assessments for SLTTs, personnel based at CISA headquarters conduct technical cybersecurity assessments. For example, the Vulnerability Management subdivision provides vulnerability scanning and risk and vulnerability assessments.

Incident Response

When ransomware incident response is requested by SLTTs, **CISA** and the MS-ISAC provide technical incident mitigation and triage, forensic analysis of system images and networks, and coordination assistance. CISA and the MS-ISAC each have 24x7 watch floors that provide situational awareness and provide incident response assistance through CISA's Threat Hunting team and MS-ISAC's Computer Incident Response Team. CISA and the MS-ISAC can help SLTTs scope the severity of their incidents and provide actionable guidance and recommendations to assist with response, containment, and remediation. They can also support SLTTs by analyzing system images and logs from network devices and security appliances for signs of malicious activity at no cost. In addition, CISA and MS-ISAC have released a ransomware guide that includes a response checklist for ransomware victims with steps to detect, contain and eradicate, and recover from ransomware.

The **FBI and Secret Service** have each issued ransomware and cybersecurity incident response guidance with recommended practices and reporting procedures. These agencies provide assistance by conducting criminal investigations and attributing attacks to threat actors when SLTTs notify them of ransomware attacks (or when they become aware of an incident through their ongoing monitoring of cyber threats and events) and SLTTs request assistance.

The FBI has the IC3, Cyber Task Forces[76] across 56 field offices throughout the country, and a 24x7 cyber operations center, referred to as CyWatch, where the agency can receive reports of or learn about cyber incidents. CyWatch reviews and shares cyber incident reports with CISA, relevant sector risk management agencies, and the FBI's Cyber Task Forces for further investigation. The FBI can also conduct assessments at its cyber operations center to determine threat levels and conduct strategic analysis to identify any potential similarities to other investigations.

The FBI encourages state and local governments to contact their local field offices in the event of a cyberattack. In addition to conducting criminal investigations for attribution, the FBI may be able to assist in recovering ransoms paid by victims and providing known encryption keys to regain access to systems and data, as appropriate. The FBI may also be able to disrupt the malicious actor's ability to access funds from ransom payments using its legal authorities.

Secret Service has 42 domestic Cyber Fraud Task Forces that partner with SLTTs and federal law enforcement agencies to share information, conduct investigations, and provide support with incident response and digital forensics. Secret Service also provides response training to state and local law enforcement through its National Computer Forensics Institute. According to the institute's officials, graduates receive about $14,000 worth of IT tools and equipment used to respond to and investigate cyber incidents within the SLTT community. Officials in Secret Service's National Computer Forensics Institute provided an example of a recent graduate who ably assisted a state. In summer 2019, the state of Louisiana issued a state of emergency when several of its networks were attacked and infected, affecting public safety and health. According to the officials, the graduate responded, limited damage, and restored the network.

In March 2021, Secret Service conducted a ransomware incident response tabletop exercise with SLTT government officials, which used a simulated scenario to enhance planning, collaboration, and information sharing between state and local government agencies and the Secret Service. According to Secret Service, the crisis role-play simulation

[76] The FBI's Cyber Task Forces are located in the agency's 56 field offices. According to the FBI, each Cyber Task Force is a multidisciplinary, cross-program, and multiagency team that synchronizes operational, intelligence, or technical efforts and roles in cyber investigations and response within its territory.

allowed participants to gain a better understanding of how to efficiently and effectively respond to a ransomware attack.

Other Federal Agencies Indirectly Support State, Local, Tribal, and Territorial Governments

Several additional federal agencies—FEMA, National Guard Bureau, NIST, and Treasury—provide indirect forms of assistance that supports SLTTs' efforts to address ransomware. Unlike CISA, FBI, and Secret Service, these federal agencies generally do not interact directly with SLTTs in preventing and responding to ransomware. However, each agency has ransomware-related initiatives or activities that may indirectly benefit SLTTs and contribute to the federal government's efforts to combat ransomware across the nation.

FEMA, with assistance from CISA, supports SLTTs' efforts to enhance their cybersecurity posture through its homeland security preparedness grant programs that include funding opportunities for cybersecurity projects. According to FEMA officials, there are six grant programs that have cybersecurity as a focus. FEMA officials stated that the funding for cyber-related projects varies annually; however, two of the grant programs required the recipients to spend at least 7.5 percent of the received funds on cybersecurity in 2021.

In addition, Congress and the President passed the *State and Local Cybersecurity Improvement Act* to establish a new grant program administered by FEMA (with assistance from CISA) relating to the cybersecurity of state and local governments.[77] The act authorized up to $1 billion to be made available to state and local agencies from fiscal years 2022 through 2025 to develop and implement a plan that addresses cybersecurity risks to their systems. Specifically, FEMA would receive applications and grant funds. CISA will provide subject matter expertise on cybersecurity, including reviewing cybersecurity plans from SLTTs that have received funding.

National Guard Bureau indirectly supports SLTTs through implementing policy and providing guidance to National Guard units. It can also help entities in hands-on ransomware prevention and response under certain

[77] *Infrastructure Investment and Jobs Act*, Pub. L. No. 117-58, div. G, title VI, subtitle B, 135 Stat. 429, 1272-1285. (Nov. 15, 2021).

limited circumstances.[78] According to National Guard officials, Title 10[79] and Title 32[80] are the primary authorities that prescribe federalized use of the National Guard, but personnel in those statuses are limited in their support to SLTTs with ransomware incidents.

The National Guard can also provide additional assistance through state- and territory-level authorities.[81] In those approved circumstances, SLTTs may also hire their state's National Guard members to provide hands-on prevention and response assistance in a state active duty status, operating as state employees under state laws.

NIST indirectly supports SLTTs by providing education and awareness on ransomware issues through its cybersecurity-related publications and guidance. For example, NIST's Special Publication 1800 series provides guidelines on an organization's security practices for their information systems to identify, protect, detect, respond, and recover from ransomware incidents.[82] Further, NIST Special Publication 1800-26 demonstrates methods and potential tool sets that can detect, mitigate, and contain data integrity events in networks as well as tools and strategies to aid in a security team's response to a data integrity event. In addition, NIST Special Publication 800-184 provides tactical and strategic guidance regarding the planning, playbook development, testing, and improvement of recovery planning for a cyber incident. It also provides an

[78] The process for requesting federal assistance is established under DOD Directives 3025.18, *Defense Support of Civil Authoritie*s and 3160.01, *Homeland Defense Activities Conducted by the National Guard.*

[79] 10 U.S.C. § 101(d) refers to "active duty" as full-time duty in the active military service. For cyber activities, this requires both DOD approval as well as network owner approval. It allows the President to "federalize" the National Guard forces by ordering them to active duty in their reserve component status or by calling them into federal service in their militia status in accordance with U.S. code sections.

[80] 32 U.S.C. § 101(19) refers to "full-time national guard duty" as training or other duty, other than inactive duty, performed by a member of the National Guard. For cyber activities, this requires both DOD approval as well as network owner approval.

[81] Depending on a state's incident response plan, the National Guard may be called upon by the governor under state active duty to directly support an SLTT affected by a ransomware attack. This may require a state official to issue an emergency declaration.

[82] National Institute of Standards and Technology (NIST), Special Publication 1800-11. *Data Integrity: Recovering from Ransomware and Other Destructive Events* (September 2020); SP 1800-25, *Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events* (December 2020); SP 1800-26, *Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events* (December 2020).

example scenario of a ransomware attack to demonstrate guidance and informative metrics that may be helpful for improving resilience of information systems.[83]

NIST also issued a cybersecurity framework profile in February 2022 specific to ransomware. The profile is intended to help organizations manage the risk of ransomware events, identify an organization's response level, and help improve on cybersecurity to prevent ransomware.[84] CISA has referred to NIST guidance on the stopransomware.gov website and in certain alerts about ransomware.

Treasury provides indirect assistance to SLTTs on ransomware by, among other things, issuing sanctions against malicious cyber actors and institutions that facilitate ransomware payments, investigating suspicious financial activity that may be related to ransomware, and tracking ransomware payments through cryptocurrency exchanges. For example, in September and November 2021 Treasury issued sanctions against cryptocurrency exchange SUEX[85] and Chatex,[86] pursuant to Executive Order 13694[87] for facilitating financial transactions involving ransomware payments from malicious cyber actors.

Additionally, in April 2022, Treasury reported that it sanctioned Hydra Market, a prominent dark web market, to disrupt proliferation of malicious cybercrime services (such as ransomware-as-a-service),[88] dangerous

[83] NIST, Special Publication 800-184, *Guide for Cybersecurity Event Recovery* (December 2016).

[84] NIST, Interagency or Internal Report 8374, *Ransomware Risk Management: A Cybersecurity Framework Profile* (February 2022).

[85] SUEX is a virtual currency exchange or platform that allows individuals to buy and sell cryptocurrency or digital currency such as Bitcoin.

[86] Chatex is a virtual currency exchange that has direct ties with SUEX and have been known to facilitate financial transactions for ransomware actors. In addition, IZIBITS OU, Chatextech SIA, and Hightrade Finance Ltd. have been sanctioned for enabling Chatex operations.

[87] The White House, *Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities,* Executive Order 13694 (Apr. 1, 2015). The executive order authorized sanctions on cyber actors determined to be responsible for or complicit in malicious cyber activities that contribute to financial payments.

[88] Ransomware-as-a-service describes a subscription-based business model that allows malicious actors, including those with little to no technical skill, to pay to launch ransomware attacks developed by operators.

drugs, and other illegal offerings available through the Russia-based site.[89] It also reported that the department identified approximately $8 million in ransomware proceeds that transited Hydra's virtual currency accounts. According to Treasury officials, the Financial Crimes Enforcement Network also supports FBI's efforts to disrupt criminal networks by participating in law enforcement investigations and sharing analysis of illicit financial activity, when appropriate.

SLTT Governments Were Generally Satisfied with Federal Ransomware Assistance, but Identified Challenges

The SLTT government officials we interviewed were generally satisfied with the prevention and response assistance from federal agencies that include CISA (and products and services that it provides through a cooperative agreement with the MS-ISAC), FBI, and Secret Service. Among other assistance, officials cited helpful ransomware guidance, detailed threat alerts, quality no-cost technical assessments, and timely incident response assistance. Although officials from SLTT governments generally had positive experiences with the federal assistance, they identified challenges related to awareness and outreach, and communication. Additionally, officials identified service enhancements, funding, and federal coordination as opportunities to improve federal assistance on ransomware.

SLTT Governments Were Generally Satisfied with Ransomware Assistance

Officials from 13 SLTTs were generally satisfied with the ransomware assistance from the federal government across four categories—education and awareness, information sharing and analysis, cybersecurity reviews and assessments, and incident response.

Education and Awareness

Twelve of the 13 SLTTs we interviewed and five of six national organizations reported that education and awareness assistance from the federal government helped them to prepare for ransomware threats. Officials noted that they participated in ransomware-related tabletop exercises, received ransomware guidance, and attended various trainings and seminars hosted by federal agencies. For example, one county mentioned that it distributed more than 140 posters, which CISA customized with unique cybersecurity best practices and incident response guidance that county officials could use to help prevent and

[89] Department of the Treasury, "Press Releases: Treasury Sanctions Russia-Based Hydra, World's Largest Darknet Market, and Ransomware-Enabling Virtual Currency Exchange Garantex," (Apr. 5, 2022), accessed May 2, 2022, https:/home.treasury.gov/news/press-releases/jy0701.

respond to incidents. In addition, a national organization stated that its SLTT members appreciated MS-ISAC's role in providing useful ransomware education, such as its ransomware readiness and prevention training, and helping SLTTs create their own training programs to improve cyber hygiene within their states.[90] Another organization stated that CISA worked directly with states to develop tailored incident response plans and tabletop exercises with real-world scenarios to enhance readiness and emphasize awareness.

Information Sharing and Analysis

Twelve of the 13 SLTTs and five national organizations reported that SLTTs were receiving information sharing and analysis assistance provided by the federal government and appreciated the timely, detailed, and quality threat information and indicators of compromise. Officials noted that assistance from the federal agencies has impacted their readiness in combatting threats such as ransomware. For example, one public school district stated that CISA's, MS-ISAC's, and FBI's alerts and advisories on advanced persistent threats and mitigation strategies increased its readiness. In addition, one national organization stated that while its SLTT members receive cyber advisories from various sources, they value and view the alerts from CISA and FBI as the most prominent. Similarly, one locality acknowledged the federal government as the honest broker of security-related information and stated that it uses CISA's alerts, advisories, and other information to help justify additional funding to address cybersecurity threats.

Cybersecurity Review and Assessment

Similarly, 12 of 13 SLTTs and four of six national organizations reported that cybersecurity reviews and assessments from the federal government helped them enhance resilience and the effectiveness of the safeguards on critical systems supporting operations. Specifically, officials reported that SLTTs received vulnerability scanning, intrusion detection systems, network monitoring tools, and other services. They cited service quality, service availability, and no-cost services as key factors for leveraging services from the federal government.

For example, seven SLTTs used MS-ISAC's malicious domain blocking tool, which can block ransomware infections by preventing the initial

[90] We asked SLTTs to provide perspectives on MS-ISAC's efforts to assist with ransomware, given its cooperative agreement with CISA.

outreach to a web domain with known threats. One locality mentioned that although it considered paying for a similar malicious domain blocking tool from a third-party vendor, it decided to go with MS-ISAC since it was free, met its needs, and had proven to be effective by blocking more than 10,000 malicious requests. In addition, one national organization stated that the tool allowed states to detect malicious activity within minutes. Lastly, another locality stated that it appreciated the no-cost assessments and the federal agencies' ability to identify vulnerabilities and weaknesses for a county supported by a single IT professional who did not always have access to such cybersecurity resources and tools.

Incident Response

In addition to receiving federal assistance to support SLTTs' ransomware prevention efforts, 11 of the 13 SLTTs and four of six national organizations reported instances where federal assistance was requested to respond to a ransomware incident within the last 4 years. SLTTs were generally satisfied with the federal assistance that they received from CISA, MS-ISAC, and Secret Service. Specifically, SLTTs generally appreciated the quality and timeliness of the response to a reported ransomware incident. For example:

- One locality emphasized that the support it received from CISA was outstanding as it responded to a ransomware incident that occurred on a Sunday morning at 4:00 a.m. The incident affected the county's core systems supporting its 911 emergency dispatch center. Local officials noted that it initially responded to the incident using tips the county learned by attending multiple CISA led seminars. Officials also stated CISA provided the county forensic and data preservation tools for the servers and helped the county determine that the malicious actors launched a ransomware attack by compromising a connection with a trusted vendor. They further noted that the malicious actors encrypted data more than three times, which made it too resource intensive to break. Officials added that CISA also helped the county terminate the connection to isolate the attack, quickly analyzed the forensic data, and provided a complete report within several hours the day of the incident.
- Similarly, a locality stated that it could not have recovered from its ransomware incident without assistance from CISA. Specifically, CISA provided remote assistance by providing the county software and detailed instructions that allowed officials to take forensic copies of the affected servers. County officials sent the forensic data to a CISA analyst for review and the analyst was able to explain what happened

and how it happened. Officials added that the locality did not have an incident response plan prior to the attack, but it has since used a template that CISA provided following the incident.

- Another locality experienced a ransomware incident that encrypted criminal justice related data and affected the county's workstations and servers supporting its 911 dispatch center that tracks the location of emergency vehicles and incoming calls for assistance. The county rerouted communications to a neighboring county to minimize the immediate impact of the incident. A local official stated that the county's IT department included one IT professional and noted that MS-ISAC's assistance shortened the downtime and allowed the county to respond without paying the ransom or a contractor for recovery services. The official also noted that MS-ISAC provided a report following the incident that summarized the attack, identified key weaknesses, and included actionable improvement activities to strengthen the county's cybersecurity posture.

SLTTs and National Organizations Identified Challenges with Federal Assistance on Ransomware

Although SLTTs were generally satisfied with ransomware prevention and response assistance, all 13 SLTTs and six national organizations cited challenges in CISA's, MS-ISAC's, and FBI's efforts. Specifically, officials cited challenges with awareness and outreach, and communication.

Awareness and Outreach

Eleven SLTTs and six national organizations reported difficulties identifying the federal prevention and response services that were available to SLTTs. For example, a locality noted that it did not always know what services and resources were available and from which agency. Similarly, two public school districts that experienced a ransomware attack stated that they were not aware of resources available to them from the federal government. One district's officials were unaware of the MS-ISAC and its services at the time of our interview with them and the other district's officials stated that they had no form of direct communication with the MS-ISAC.

Three SLTTs stated that they were unaware of CISA's regional personnel, including cybersecurity advisors and protective security advisors, who conduct outreach and can provide cyber and physical security services to SLTTs. This includes tribal officials who stated that they were not aware of CISA's regional personnel or its role in working with tribal nations. Tribal officials expressed concerns about CISA's focus on conducting outreach at the state level leaving tribal nations uninformed as they are independent from the state and would not be aware of interactions or decisions with CISA. According to CISA, it is happy to engage directly with tribal nations to offer support and services. CISA also stated that its continued engagement with organizations such as TribalNet, the Department of the Interior's Bureau of Indian Affairs, the National Indian Gaming Commission, and others help it engage tribal nations and provide information regarding available resources.

Further, officials had difficulties in identifying the roles, responsibilities, and expectations of each agency with respect to ransomware. For example, a national organization mentioned that among its members, there was no clarity at the state level about federal agency roles to know who does what and when in the event of a ransomware attack on an SLTT.

Similarly, the lack of clarity in the FBI's role has led to confusion among SLTTs. For example, one locality reached out to the FBI to establish a relationship in the event it experienced a ransomware incident, but only received information related to its investigative role for election security causing confusion. Three additional localities were generally unaware that the FBI did not offer hands-on services causing them to reach out to another entity for assistance. According to the FBI, its engagements with cyber incident victims are generally limited to evidence collection and, on occasion, technical operations, which might involve some hands-on work to advance counter threat objectives. As of July 2022, the FBI's incident response guidance did not specify that such hands-on assistance is available to help SLTTs respond to cyber incidents, including ransomware.

Communication

Twelve SLTTs and three national organizations also reported that federal agencies had inconsistently communicated with SLTTs during incident response efforts. For example, a locality noted that federal agencies failed to communicate information regarding a ransomware incident that affected 23 organizations across the state. According to local officials, the incident impacted the public facing webpage that supports early voting by allowing citizens to lookup records and locate the right precinct. While the locality was very satisfied with MS-ISAC's and FBI's initial efforts to help resolve the incident, local officials stated that they did not provide enough information regarding the attack and the county learned more information through the media than directly from the federal government. According to the FBI, it has a statutory obligation to protect victim data and preserve the integrity of investigations. The Bureau also stated that its ability to share information during active investigations is limited, but it will share information to the extent possible.

While there were several instances where SLTTs felt supported by the FBI during their ransomware incidents, six of the 12 respondents who contacted the FBI for response assistance cited inconsistent communication. Although the FBI has a lead investigative role, SLTTs found that the FBI either collected evidence without further communication, did not provide timely assistance, or did not respond at all to SLTT requests for assistance with a ransomware incident.

For example, one respondent noted that when they called the FBI's 24-hour incident response number, it went immediately to voicemail and the agency never responded to the reported ransomware incident. The respondent's incident was determined to originate from a foreign nation state actor, which falls within the FBI's role and responsibility with respect to ransomware. However, its lack of a response back to the SLTT limited the locality's ability to analyze the incident. At the time of our interview, it had been 8 months since the SLTT had contact with the FBI regarding its ransomware incident.

Two additional respondents noted that the FBI collected evidence, one of which involved a foreign nation state actor, but did not offer to provide additional assistance to respond to the ongoing ransomware incident or follow-up with the results of their investigation. The SLTTs added that they had expected the FBI to provide information about the attack that could be used in their own analysis. While the FBI stated that it shares as much information as allowed by policy, in these instances the SLTTs did not fully understand the FBI's limitations.

Another locality stated that while it contacted the local FBI field office the day of an incident, the agency did not respond until after the incident was resolved 2 weeks later. Further, another locality decided not to contact the FBI for assistance with its ransomware incident affecting criminal justice related data due to the lack of response to the locality's prior request to the FBI to begin receiving InfraGuard alerts. The FBI acknowledged that prompt feedback is a challenge due to various factors including efforts to incorporate evidence into broader ongoing investigations and coordination with federal and non-federal entities.

SLTTs and National Organizations Identified Opportunities for Improving Federal Assistance on Ransomware

Based on their experiences, officials from SLTTs and national organizations identified opportunities for improving federal assistance on ransomware. Among other suggestions, officials called for federal agencies to enhance services, provide opportunities for additional funding, and centralize federal coordination.

Service Enhancements

Nine of the 13 SLTTs and three of six national organizations recommended that CISA and MS-ISAC provide more tailored services for smaller localities with limited resources and to further enhance the cybersecurity assessments and tools. For example, officials suggested enhancements to the malicious domain blocking tool to fit in a remote work environment, tools for running phishing exercises, vulnerability assessments with increased depth, and low cost or bulk options for deploying intrusion detection sensors. According to CISA, the agency plans to offer additional services to smaller SLTTs and such efforts would allow SLTTs with low resources to receive the same information and situational awareness.

Additionally, a locality noted that it would like for CISA or FBI to enhance their information sharing capabilities by reviewing the dark web to gain intelligence. The locality also stated that reviewing the dark web would help to identify a list of soft SLTT targets to prioritize outreach efforts and prevention services. According to local officials, its school district fell victim to a ransomware attack because adversaries used the dark web to identify it as a soft target. Officials added that taking such a proactive approach would greatly benefit small localities who may not have the expertise to collect intelligence from the dark web.[91]

According to the FBI, the agency at times will provide proactive information to entities directly, publicly, or through other agencies. For example, the FBI may directly reach out to entities when specific intelligence or other threat information arises in an investigation or possibly from the dark web. This intelligence and other information is shared for prevention or mitigation purposes and may assist in asset

[91] The *Cyber Incident Reporting for Critical Infrastructure Act of 2022* enacted as division Y of the *Consolidated Appropriations Act 2022,* called for CISA to establish a ransomware vulnerability warning pilot program by March 2023. The program is to help develop procedures for identifying information systems that contain security vulnerabilities associated with common ransomware attacks, and to notify the owners. The act does not explicitly require CISA to use information from the dark web as part of the ransomware warning pilot program.

recovery and restoring data. Nonetheless, in this instance, the locality reported that it did not receive threat information from a federal agency prior to its attack and suggested such information be used to prioritize federal outreach efforts.

Funding

Five of the 13 SLTTs and all six national organizations noted that additional funding would better equip them to address cybersecurity concerns and build resilience against threats, including ransomware. Officials stated that they do not have the budget to deploy additional intrusion detection sensors, hire technical staff who can provide hands-on response assistance, address gaps identified by technical assessments, or implement safeguards recommended by federal guidance to combat ransomware.[92]

Federal Coordination

Seven of the 13 SLTTs and four of six national organizations also identified areas for central federal coordination. Specifically, they believed that there should be a central point of contact for ransomware issues. They also noted that a single catalog of available ransomware services, guidance, and roles and responsibilities across the federal government would be useful and help to clarify the assistance that is available to SLTTs. For example, one state official noted that each of the federal agencies that assist states and local governments with ransomware all have separate missions. Given this, the official commented that there is a need for less duplication with the alerts and services and greater collaboration and coordination to target localities. Additionally, an official expressed concerns regarding turnover at CISA in recent years and the impact this could have on prioritizing assistance to SLTT governments. They supported prioritizing assistance with funding to the MS-ISAC as its mission is to assist SLTTs with proactively safeguarding their systems against emerging threats.

Although CISA developed www.stopransomware.gov in collaboration with other federal agencies to serve as a central repository of federal guidance, alerts, and other information, officials cited difficulties in

[92] As previously mentioned, the *State and Local Cyber Improvement Act* authorized funding of up to $1 billion between fiscal years 2022 and 2025 through a grant program. If appropriated, this could help SLTTs address cybersecurity issues, including combatting ransomware. This act was passed after we concluded our interviews with SLTTs.

navigating the website. One local official stated that SLTTs should be able to pull up guidance quickly. The official's impression was that one had to click on as many as 20 links to find the information needed.

SLTTs also cited instances of duplicative and inefficient efforts between federal agencies when responding to ransomware incidents. For example, one school district official noted that in response to a ransomware incident, the FBI asked for the same forensic information as CISA. The official added that the request was duplicative and the state directed the FBI to collaborate and contact CISA for the data since the school district does not have the capacity to fulfill multiple requests for the same information.[93] In addition, when we asked SLTTs which federal agencies they contacted to receive assistance, nine of 13 SLTTs stated that they had to contact more than one federal agency to notify them about the incident and/or receive federal assistance.[94]

Federal Agencies Partially Addressed Most Key Collaboration Practices

CISA, FBI, and Secret Service have existing collaborative mechanisms and have coordinated on certain ransomware assistance, such as developing a website. However, the agencies have not addressed aspects of six of seven key collaboration practices, such as defining outcomes and developing written guidance and agreements.

CISA, FBI, and Secret Service Have Existing Collaborative Mechanisms and Have Coordinated on Certain Ransomware Assistance

CISA, FBI, and Secret Service have several existing mechanisms that can facilitate cyber incident coordination with other federal agencies, including SLTT support on ransomware incidents. For example:

- **Agency detailees.** CISA, FBI, and Secret Service utilize interagency detailees, or personnel who represent their agency by being co-located at a partnering organization, to facilitate coordination. Specifically, according to CISA, the agency hosts three detailees from the FBI and one detailee from Secret Service. Additionally, CISA

[93] CISA and FBI acknowledged that duplicative efforts to collect evidence may occur in some cases, despite federal coordination, to maintain a clear chain of custody or movement of evidence for information that may support ongoing investigations within the FBI.

[94] We asked the 13 SLTT government entities a question regarding which federal agencies, if any, they contacted when they experienced a ransomware incident. We did not ask this question of the six national organizations we interviewed because it was not applicable to them.

officials noted that detailees are able to access officials, resources, and databases of the host agency to improve information sharing and response efforts from their respective agency in coordinating and addressing SLTT needs.

- **Field-level staff and task forces.** In addition, the three agencies have field-level staff and task forces that can coordinate with other federal agencies through informal means. According to CISA, the agency has 57 regional cybersecurity advisors[95] that provide field-level assistance to SLTTs, and FBI and Secret Service have cyber task forces in place at their field offices throughout the country that are intended to provide field-level response to cyber incidents.[96] For example, the FBI has cyber task forces located in the agency's 56 field offices that are to synchronize domestic cyber threat investigations in the local community through information sharing, incident response, and joint enforcement and intelligence actions. Similarly, Secret Service has 42 domestic cyber fraud task forces, which serve as the field-level focal point of cyber investigative efforts to help combat cybercrime through prevention, detection, mitigation, and investigation.

  According to agency officials, when an SLTT requests assistance from CISA's regional cybersecurity advisors or from FBI or Secret Service field offices, the federal agency that receives the request typically determines the next steps to assist the SLTT, including whether to involve other federal agencies. For instance, according to CISA officials, the agency may collect initial technical information about the attack and help the SLTT to diagnose where the attacker initially infiltrated its systems. Additionally, CISA noted that upon request, the agency may also refer SLTT partners to FBI or Secret Service at their location to assist with any potential criminal investigation.

Further, CISA, FBI, and Secret Service have demonstrated efforts to coordinate on certain ransomware assistance to SLTTs. For example:

[95] According to CISA, the total of regional cybersecurity advisors includes 10 Chiefs of Cybersecurity who supervise 38 Cybersecurity State Coordinators and nine Regional Cybersecurity Advisors.

[96] According to CISA, the agency's cybersecurity advisors perform and coordinate cyber security assessments for all 16 critical infrastructure sectors, including state, local, tribal, and territorial governments.

- As previously mentioned, CISA, in coordination with FBI, Secret Service, and other federal partners, established a website—www.stopransomware.gov—that provides a central repository for ransomware-related resources. The website is intended to improve SLTTs' awareness of federal ransomware-related resources, such as contact information for federal agencies and a ransomware guide that provides ransomware prevention best practices, as well as a checklist for responding to ransomware incidents.
- These agencies have also participated in joint events, such as Secret Service's ransomware tabletop exercise.[97] They have also issued several joint guidance documents, alerts, and advisories on ransomware threats, which can help to improve SLTT's awareness and preparedness. For example, in February 2021 the National Cyber Investigative Joint Task Force (NCIJTF)[98] released interagency ransomware prevention and response guidance for SLTTs cosigned by over 15 other federal agencies, including CISA and Secret Service.[99] In addition, as previously mentioned, CISA issued 17 joint alerts and advisories in partnership with FBI, Secret Service, and other federal and international entities, as of June 2022.

Agencies' Ransomware Coordination Generally Addressed Only One of Seven Key Practices

While having existing collaborative mechanisms and having demonstrated instances of coordination are positive steps, CISA, FBI, and Secret Service have not addressed aspects of six of seven key practices for interagency collaboration in their ransomware assistance to SLTTs.

Specifically, CISA, FBI, and Secret Service generally addressed one practice, partially addressed five practices, and did not address one practice. Table 2 summarizes the extent to which the federal agencies

[97] A tabletop exercise brings people together to introduce, talk through, and explore how they would respond to simulated scenarios addressing potential threats.

[98] The FBI's NCIJTF is a multiagency cyber center that serves as the national focal point for whole-of-government campaigns against cyber threats and adversaries. Among other things, it is responsible for coordinating, integrating, and sharing information on cyber threat investigations. It also synchronizes joint efforts across over 30 partnering agencies from across law enforcement, the intelligence community, and the federal government—including CISA and Secret Service—that focus on identifying and pursuing malicious actors.

[99] FBI, NCIJTF, *Ransomware: What It Is & What To Do About It* (February 2021), https://www.ic3.gov/Content/PDF/Ransomware_Fact_Sheet.pdf.

addressed key practices for interagency collaboration in their ransomware assistance to state and local governments.[100]

Table 2: Extent to Which the Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation, and Secret Service Addressed Key Collaboration Practices in Their Ransomware Assistance to State and Local Governments

Key practice	Key considerations	Extent addressed
Defining outcomes and monitoring accountability	Have short-term and long-term outcomes been clearly defined? Is there a way to track and monitor progress toward the short-term and long-term outcomes?	Not addressed
Bridging organizational cultures	What are the missions and organizational cultures of the participating agencies? Have participating agencies developed ways for operating across agency boundaries?	Partially addressed
Identifying and sustaining leadership	Have agency leads or individuals been clearly identified?	Generally addressed
Clarifying roles and responsibilities	Have participating agencies clarified the roles and responsibilities of the participants? Have participating agencies articulated and agreed to a process for making and enforcing decisions?	Partially addressed
Including relevant participants	Have all relevant participants been included? Do the participants have the ability to regularly attend activities of the collaborative mechanism?	Partially addressed
Identifying and leveraging resources	How will the collaborative mechanism be funded or staffed? Have participating agencies developed online tools or other resources that facilitate joint interactions?	Partially addressed
Developing and updating written guidance and agreements	Have participating agencies documented their agreement regarding how they will be collaborating? Have they developed ways to continually update or monitor written agreements?	Partially addressed

Legend: Generally addressed = agencies addressed selected key considerations for the key practice; Partially addressed = agencies addressed some, but not all aspects of the selected key considerations for the key practice; Not addressed = agencies did not address the selected key considerations for the key practice

Source: GAO analysis of agency documentation. I GAO-22-104767

Defining outcomes and monitoring accountability. CISA, FBI, and Secret Service acknowledged that they have not jointly developed short-term and long-term outcomes for providing ransomware assistance to SLTTs and ways to track and monitor their progress. The agencies reported that they established their own outcomes for internal ransomware initiatives. For example, Secret Service officials noted short-term and long-term outcomes for its SLTT training efforts through the National Computer Forensics Institute, which is operated by Secret

[100] We included all seven key practices for interagency collaboration in our review. For certain practices, we only evaluated aspects of the practice that were relevant.

Service's Office of Investigations, to equip detailees and other federal agencies with the necessary training and equipment to respond to SLTT cyber incidents. Additionally, the FBI, through the NCIJTF, developed a Counter-Ransomware Concept of Operations to support the National Security Council's U.S. Counter-Ransomware Campaign Plan.[101] Further, in our interviews with officials from CISA, they identified long-term goals that the agency had for disrupting the ransomware business model and equipping SLTTs with the resources and information they need to defend themselves. However, none of these initiatives defined outcomes or monitoring mechanisms for providing and coordinating ransomware assistance to SLTTs among the three agencies.

Bridging organizational cultures. CISA, FBI, and Secret Service have partially addressed this practice by identifying commonalities and differences in their missions through initiatives, as well as alerts and guidance. Initiatives such as the FBI's NCIJTF and CISA's Joint Cyber Defense Collaborative (JCDC) focus on a whole-of-government approach to addressing cyber risks and threats, including ransomware, through information sharing and coordination.[102] Additionally, the three agencies established ways to operate across agency boundaries through interagency detailees, as well as field-level staff and task forces.

However, these mechanisms did not address aspects of the practice on bridging organizational cultures as it relates to federal ransomware assistance to SLTTs. Specifically, the FBI's NCIJTF and CISA's JCDC were not being used as mechanisms to coordinate federal agencies' assistance on SLTT incidents. Rather, these mechanisms were addressing broader, whole-of-government strategic approaches to

[101] The NCIJTF's Counter-Ransomware Concept of Operations states that the document complements the U.S. Counter-Ransomware Campaign Plan and provides a framework for the coordination of counter-ransomware activities. According to the Concept of Operations, the NCIJTF is to support the National Security Council in the implementation of the U.S. Counter-Ransomware Campaign Plan by leveraging its existing coordination framework for whole of government cyber campaigns. Officials from the National Security Council noted that the U.S. Counter-Ransomware Campaign Plan is in draft and did not provide time frames for its completion.

[102] CISA's JCDC is to help unify defensive actions and drive down risk in advance of cyber incidents. It includes the public and private sectors as well as SLTT governments and federal representatives, such as FBI and Secret Service, to strengthen the nation's cyber defenses through innovative collaboration, advanced preparation, and information sharing and fusion.

improve information sharing on ransomware threats and to disrupt IT infrastructure and criminal networks that enable ransomware.

Specifically, according to CISA, the JCDC is in the process of developing a formalized Ransomware Collaboration Framework for ransomware information sharing and disruption, which is to be focused specifically on ransomware activity with the potential for national impact. Additionally, CISA officials noted that the goal of the framework is to create an outline for how the JCDC plans to share, coordinate, and operationalize ransomware threat information for a long-term mitigation strategy that will greatly disrupt the threat of ransomware and thereby increase the security and resilience of U.S. critical infrastructure and national interests. According to FBI officials, the FBI's CyWatch—a 24x7 operations center that monitors cybersecurity activity—shares cyber incident reports with CISA. However, its CyWatch procedures did not address how this mechanism coordinates SLTT response assistance.

In addition, although FBI and Secret Service have detailees assigned to CISA and PPD-41 outlines their roles, the three federal agencies did not have procedures for how coordination should occur on SLTT assistance, which could result in certain agencies being delayed in their responses or duplication of efforts. Further, FBI and Secret Service did not host agency-level or field-level detailees with each other or from CISA who are tasked with coordinating on SLTT requests for ransomware assistance. According to FBI officials, in October 2020, FBI and CISA established a pilot program that stations CISA's regional personnel such as cybersecurity advisors at two FBI field-level task forces to enhance and expedite coordination among these agencies. However, FBI officials stated that CISA and FBI have not assessed the effectiveness of the pilot or determined whether the field-level detailees would become a normal part of their operations.

Identifying and sustaining leadership. CISA, FBI, and Secret Service generally addressed this practice by documenting the agency leads for ransomware prevention and response activities in a joint ransomware guide and fact sheets available on www.stopransomware.gov. As previously stated, per PPD-41, DHS, through CISA, is the lead federal agency for asset response (e.g., technical analysis and mitigation) and DOJ, through the FBI and NCIJTF, is the lead agency for threat response (e.g., law enforcement and attribution of threat actors) to cyber incidents. The agency leads identified for ransomware prevention and response assistance are consistent with PPD-41. Officials from Secret Service noted that it partners with CISA, FBI, and NCIJTF to support their asset and threat response efforts.

Clarifying roles and responsibilities. CISA, FBI, and Secret Service partially addressed this practice by identifying the roles and responsibilities for assisting SLTTs with ransomware in a joint ransomware guide and in publicly available fact sheets. However, FBI and Secret Service have not clarified for SLTTs how their roles as investigative leads differ related to ransomware response activities. Further, the three agencies have not demonstrated that they jointly agreed on a process for making decisions when collaborating on ransomware assistance. For example, the three agencies did not establish a process for how and when to alert and involve another federal agency on an SLTT reported ransomware incident. Thus, the decision to involve another federal agency may not always be consistent or coordination may not occur as expected. Further, once another federal agency is involved, the decision making process between the two agencies remains unclear due to the lack of agreed upon incident handling procedures.

Including relevant participants. CISA, FBI, and Secret Service partially addressed this practice by including detailees and participating in NCIJTF, JCDC, and other agency-level cybersecurity coordination activities, including exercises and publishing joint cyber threat information products shared with SLTTs. However, not all mechanisms supported coordination on SLTT requests for assistance, or included all relevant participants. For example, while the NCIJTF and JCDC included initiatives and campaigns that focus on a whole-of-government approach to cyber risks and threats, they did not coordinate SLTT requests for assistance.

Similarly, FBI stated that information shared between the FBI's CyWatch and CISA's 24x7 cyber monitoring center helped the agencies to coordinate on cyber incident awareness more broadly, but procedures did not address how these mechanisms coordinate SLTT response assistance. Additionally, while CISA hosted agency-level detailees from FBI and Secret Service and allowed detailees to participate in daily briefings and other meetings, CISA did not host detailees from other agencies at field-level locations and has not demonstrated that it uses another mechanism to coordinate field-level SLTT assistance across agency boundaries. In addition, FBI and Secret Service did not host agency-level or field-level detailees among the three agencies to coordinate SLTT requests for ransomware assistance.

Identifying and leveraging resources. CISA, FBI, and Secret Service partially addressed this practice by having committed agency resources and jointly agreeing to host or provide interagency detailees who work within partnering federal agencies. However, the agencies have not demonstrated that they have a process for determining staffing needs (e.g., the number of detailees) to support those collaborative efforts. In addition, as previously mentioned, FBI and Secret Service did not host agency-level or field-level detailees among the three agencies to coordinate SLTT requests for ransomware assistance. It was not clear whether FBI and Secret Service considered the costs and benefits of hosting such resources.

Further, CISA, FBI, and Secret Service have not identified opportunities for leveraging collaboration tools. According to agency officials, CISA and FBI maintained separate systems to track reported incidents from SLTTs. For example, the FBI developed CyWatch, a 24x7 operations center for cyber intrusion prevention and response. CyWatch is to monitor and receive reports and follow up with appropriate components within the FBI and other federal agencies for actions related to cyber incidents.

Additionally, the FBI established CyNERGY, an interagency database and coordination platform that offers federal cyber centers and other sector risk management agencies[103] the ability to enter, view, and coordinate a whole-of-government response to targeted entities and victims of malicious cyber incidents. According to the FBI, while select early adopters used the platform, CISA and other relevant agencies did not use it.[104] Further, CISA was in the process of piloting a dashboard to track reported ransomware incidents. While interagency detailees reported that they provided input weekly during daily planning calls and ad hoc meetings or have access to these various systems, the systems did not share information on SLTT requests directly with other agencies and were not interconnected.

Additionally, according to CISA officials, its partners participated in a JCDC-hosted real-time collaboration platform to share information about ransomware, malicious cyber activity that enables ransomware infections,

[103] Sector risk management agencies are to lead, facilitate, and support, the security and resilience programs and associated activities of their designated critical infrastructure sector.

[104] The FBI is in the process of establishing CyNERGY access for federal government agencies directly supporting the national cybersecurity mission.

and other cyber threats. CISA also stated that its partners coordinate on specific ransomware incidents, including those reported by SLTT governments to CISA or other agencies. However, CISA did not provide evidence demonstrating that the platform was used to coordinate SLTT requests for ransomware assistance.

Developing and updating written guidance and agreements. CISA, FBI, and Secret Service partially addressed this practice by establishing memorandums of understanding that identify shared interagency resources through detailees and documented agency leads for ransomware prevention and response activities. However, the agencies had not developed supporting coordination procedures or other joint agreements that address actions associated with the other key practices. For example, as mentioned previously, the agencies did not document outcomes for their collaborative efforts on ransomware assistance to SLTTs, procedures for operating across boundaries through detailees and field-level staff, and processes for making decisions when providing assistance. Further, the agencies did not jointly agree on an approach for monitoring and updating agreements.

Agencies Identified Various Perspectives on Efforts to Target Ransomware, but Lacked a Mechanism to Facilitate Effective Coordination

The shortfalls across the six collaboration practices were due to the lack of a mechanism that facilitates coordination of federal agencies' ransomware assistance to SLTTs consistent with key practices. Further, existing interagency collaboration for SLTT assistance was informal and lacked detailed procedures. For example, officials stated that coordination occurred on an as-needed basis between agency detailees and field personnel.

The agencies provided a variety of perspectives on their use of informal and ad hoc processes, and broader efforts to target ransomware. Secret Service officials noted that more detailed agreements or procedures could inhibit creative freedom during investigations across its field offices. However, agency detailees noted that guidance and agreements could help them clarify points of contact for specific types of assistance and benefit overall facilitation of interagency collaboration.

Additionally, CISA noted that while NCIJTF's and JCDC's plans were not focused specifically on coordinating federal assistance on SLTT incidents, using these mechanisms to address broader strategic approaches also benefited all stakeholders, including SLTT governments. For example, CISA stated that it routinely received tips through JCDC from industry, federal government, and international partners regarding organizations (including SLTTs) that may be compromised or have a vulnerability which could subject them to an imminent ransomware attack. CISA explained that this information enabled them to quickly notify the appropriate SLTT organizations. We acknowledge that broader federal strategies to share cyber threat information and disrupt ransomware through the NCIJTF, JCDC, and other initiatives are important and can benefit a variety of stakeholders, including SLTTs. However, there have been reports of at least 867 ransomware attacks against SLTTs in the last 6 years. SLTTs could benefit from federal agencies' adoption of key practices to enhance federal coordination when assisting SLTTs on ransomware incidents.

CISA also stated that while processes were not in place that are specific to ransomware incidents, all of the agencies collaborated and responded to incidents based on PPD-41 and the threat and asset response roles established by the directive, which is discussed in its ransomware guide. CISA further noted that CISA, FBI, and Secret Service routinely coordinated and shared information as it relates to ransomware incidents, as demonstrated through their joint publications.

However, as previously mentioned, PPD-41 is intended to be a framework that supports policies, procedures, and mechanisms to be established by relevant federal agencies. CISA's ransomware guide and other relevant documentation did not detail processes demonstrating how coordination on SLTT assistance is to occur with other federal agencies. We acknowledge that the three agencies have taken steps to coordinate through efforts such as the joint ransomware website and joint guidance documents, alerts, and advisories on ransomware threats. However, we maintain that the coordination was informal and not fully consistent with key practices.

CISA agreed that the three agencies could use existing mechanisms, such as its JCDC, to better define outcomes and coordinate ransomware assistance to SLTTs. Additionally, the FBI acknowledged that there was a lack of protocols to coordinate SLTT assistance and stated that there were opportunities to improve how FBI's and CISA's cyber centers coordinate cyber incident awareness and response efforts.

The FBI stated that in addition to PPD-41, the Bureau had documented procedures to support interagency collaboration. Specifically, the FBI noted that its Domestic Investigations and Operations Guide and the Attorney General's Guidelines for Domestic FBI Operations included procedures for coordinating with other federal agencies, SLTTs, and victims. While both documents contained information regarding authorities, internal requirements, and guidelines for providing assistance to federal agencies and SLTTs, they did not outline procedures for how the coordination is to occur.

In addition, as previously mentioned, more than half of the SLTTs we interviewed identified various challenges and opportunities for further improvement when providing ransomware assistance. For example, as previously discussed, most of the SLTTs that we interviewed experienced inconsistent communication and identified opportunities to address inefficient and potentially duplicative efforts. As another example, SLTTs commented on what they viewed as a need to centralize aspects of federal coordination and services, and to further clarify assistance that each agency can provide. By addressing key practices through developing coordination procedures, enhancing collaborative tools, clarifying decision making processes and agency roles during incident response, and reinforcing accountability through joint outcomes, federal agencies could help to reduce these and other concerns cited by SLTTs. Moreover, addressing the key practices for interagency collaboration through appropriate mechanisms can help ensure more effective federal coordination on ransomware assistance to SLTTs.

Recent Law May Provide a Mechanism to Improve Federal Coordination on Ransomware

The *Consolidated Appropriations Act, 2022* includes requirements for additional federal coordination in addressing ransomware threats.[105] The act requires the Director of CISA, in consultation with the National Cyber Director, the Attorney General, and the Director of the FBI, to establish and chair a Joint Ransomware Task Force by no later than September 11, 2022. Among other things, the task force is to

- coordinate an ongoing nationwide campaign against ransomware attacks,
- consult with relevant private sector and SLTT governments and international stakeholders to identify needs and establish mechanisms for providing input into the task force, and
- facilitate coordination and collaboration between federal entities and other relevant entities to improve federal actions against ransomware threats.

Once the Joint Ransomware Task Force is established, federal agencies like CISA, FBI, and Secret Service may have a mechanism that is well positioned for coordinating federal ransomware assistance to SLTTs. It

[105] *Consolidated Appropriations Act, 2022*, Pub. L. No. 117-103, div. Y, § 106, 136 Stat. 49, 1056-57 (Mar. 15, 2022).

will be important for these agencies to address key practices for interagency collaboration in concert with the new task force to help ensure effective coordination on ransomware assistance to SLTTs.

Conclusions

Ransomware has become one of the most serious and concerning cybersecurity threats to organizations of all sizes and industries. SLTTs have been particularly targeted by ransomware attacks, which can have devastating impacts on the normal course of vital government operations and services. Consequently, the federal assistance provided directly to SLTTs to address ransomware threats is essential to enhancing cybersecurity resiliency and effectiveness in preventing and responding to related incidents. Additionally, federal agencies' broader efforts to disrupt ransomware, which provide a more indirect benefit to SLTTs, also play an important role in combatting this growing and evolving threat.

While SLTTs were generally satisfied with federal ransomware assistance they also cited a number of ways to improve federal services, outreach, communication, and coordination. Several federal agencies acknowledged that their efforts in these respects could be improved. By taking such actions, the federal government has the opportunity to further strengthen the assistance it provides to the tens of thousands SLTT organizations.

To their credit, federal agencies have coordinated on ransomware assistance to SLTTs and designated leads for technical- and law enforcement-related response. However, the agencies have not addressed aspects of other key collaboration practices such as defining common outcomes for ransomware assistance to SLTTs, procedures for how detailees should coordinate, and processes for making decisions such as how and when to involve another federal agency on a ransomware incident. These and other shortfalls were due, in part, to the lack of an established mechanism for interagency collaboration. Federal action to better address key practices for interagency collaboration will help better support the effective coordination that SLTTs need to address the pervasive ransomware threat.

Recommendations for Executive Action

We are making a total of three recommendations, two to the Department of Homeland Security and one to the Attorney General.

The Secretary of Homeland Security should direct the Director of CISA to (1) evaluate how to best address concerns raised by SLTTs and facilitate collaboration with other key ransomware stakeholders taking into account its leadership of the new joint ransomware task force and (2) improve interagency coordination on ransomware assistance to SLTTs. (Recommendation 1)

The Secretary of Homeland Security should direct the Director of Secret Service to (1) evaluate how to best address concerns raised by SLTTs and facilitate collaboration with other key ransomware stakeholders and (2) improve interagency coordination on ransomware assistance to SLTTs. (Recommendation 2)

The Attorney General should direct the Director of FBI to (1) evaluate how to best address concerns raised by SLTTs and facilitate collaboration with other key ransomware stakeholders and (2) improve interagency coordination on ransomware assistance to SLTTs. (Recommendation 3)

Agency Comments and Our Evaluation

We provided a draft of this report to the Department of Commerce (and its component agency, NIST), Department of Defense (and its component agency, NGB), DHS (and its component agencies CISA, FEMA, and Secret Service), DOJ (and its component agency, FBI), and Treasury for review and comment. We received written comments from DHS that are reproduced in appendix I and summarized below. We also received comments from an audit liaison specialist in DOJ's Justice Management Division via email stating that the department concurred with the recommendation to the FBI. In addition, DHS (including CISA, FEMA, and Secret Service), DOJ (including FBI), NGB, NIST, and Treasury provided technical comments, which we incorporated as appropriate.

In its written comments, DHS agreed with our two recommendations to CISA and Secret Service. DHS stated that CISA plans to use existing and planned efforts to address challenges and improvement opportunities identified by SLTT governments. Such efforts include addressing questions and providing information on available resources to SLTT organizations through CISA's dedicated SLTT Partnerships team and field-based cyber state coordinators. In addition, CISA is considering additional service offerings through the MS-ISAC cooperative agreement that may help smaller entities with limited resources.

DHS further noted that it remains committed to supporting SLTT governments through various collaborative mechanisms, such as the JCDC, NCIJTF, interagency liaisons, and a new Joint Ransomware Task Force. The department stated that the Joint Ransomware Task Force is to be co-chaired by CISA and FBI and include participation from Secret Service. In addition, DHS stated that the task force will examine opportunities to enhance coordination on ransomware assistance to

SLTTs through closer collaboration with interagency partners and other stakeholders on information sharing, analysis, and incident response. If implemented effectively, the actions the DHS described would address the intent of our recommendations.

While the department concurred with our two recommendations, it expressed concerns with our assessment that CISA partially addressed the key interagency collaboration practice associated with including all relevant participants in ransomware assistance to SLTT governments. DHS stated that NCIJTF and JCDC address broader, strategic approaches to ransomware while also providing a venue to coordinate on specific ransomware incidents impacting SLTT organizations. DHS further commented that CISA routinely shares information with partners and receives tips through these venues, which in turn allows the agency to offer assistance intended to prevent ransomware attacks that could affect SLTT organizations.

As discussed in this report, we acknowledge that broader federal strategies to share cyber threat information and disrupt ransomware through the NCIJTF, JCDC, and other initiatives are important and can benefit a variety of stakeholders, including SLTTs. Our assessment of the extent to which CISA addressed each key interagency collaboration practice was based on how the agency coordinated with FBI and Secret Service in providing assistance to SLTT governments. We determined that CISA had partially addressed this practice by including detailees and participating in NCIJTF, JCDC, and other agency-level cybersecurity coordination activities, such as conducting exercises and publishing joint cyber threat information products shared with SLTTs.

However, there were gaps in CISA's efforts to include relevant participants on certain SLTT assistance. For instance, CISA, FBI, and Secret Service officials who were involved with JCDC and NCIJTF previously told us that these mechanisms were not being used to coordinate interagency ransomware assistance to SLTT governments. While JCDC and NCIJTF may provide a venue for such coordination, DHS did not provide supporting documentation to demonstrate interagency collaboration among CISA, FBI, and Secret Service on ransomware response efforts for incidents affecting SLTTs.

Additionally, as we discuss in this report, CISA hosted agency-level detailees from FBI and Secret Service and allowed detailees to participate in daily briefings and other meetings. However, CISA did not host detailees from other agencies at field-level locations and has not demonstrated that it uses another mechanism to coordinate field-level SLTT assistance across agency boundaries. Thus, we maintain that our determination that CISA has partially addressed the interagency collaboration practice of including relevant participants is appropriate. Addressing the key practices for interagency collaboration through appropriate mechanisms can help ensure more effective federal coordination on ransomware assistance to SLTTs.

As agreed with your office, unless you publicly announce the contents of this report earlier, we plan no further distribution until 20 days from the report date. At that time, we will send copies to the appropriate congressional committees, the Secretaries of the Departments of Commerce, Defense, Homeland Security, and the Treasury; Attorney General of the United States, and other interested parties. In addition, the report is available at no charge on the GAO website at http://www.gao.gov.

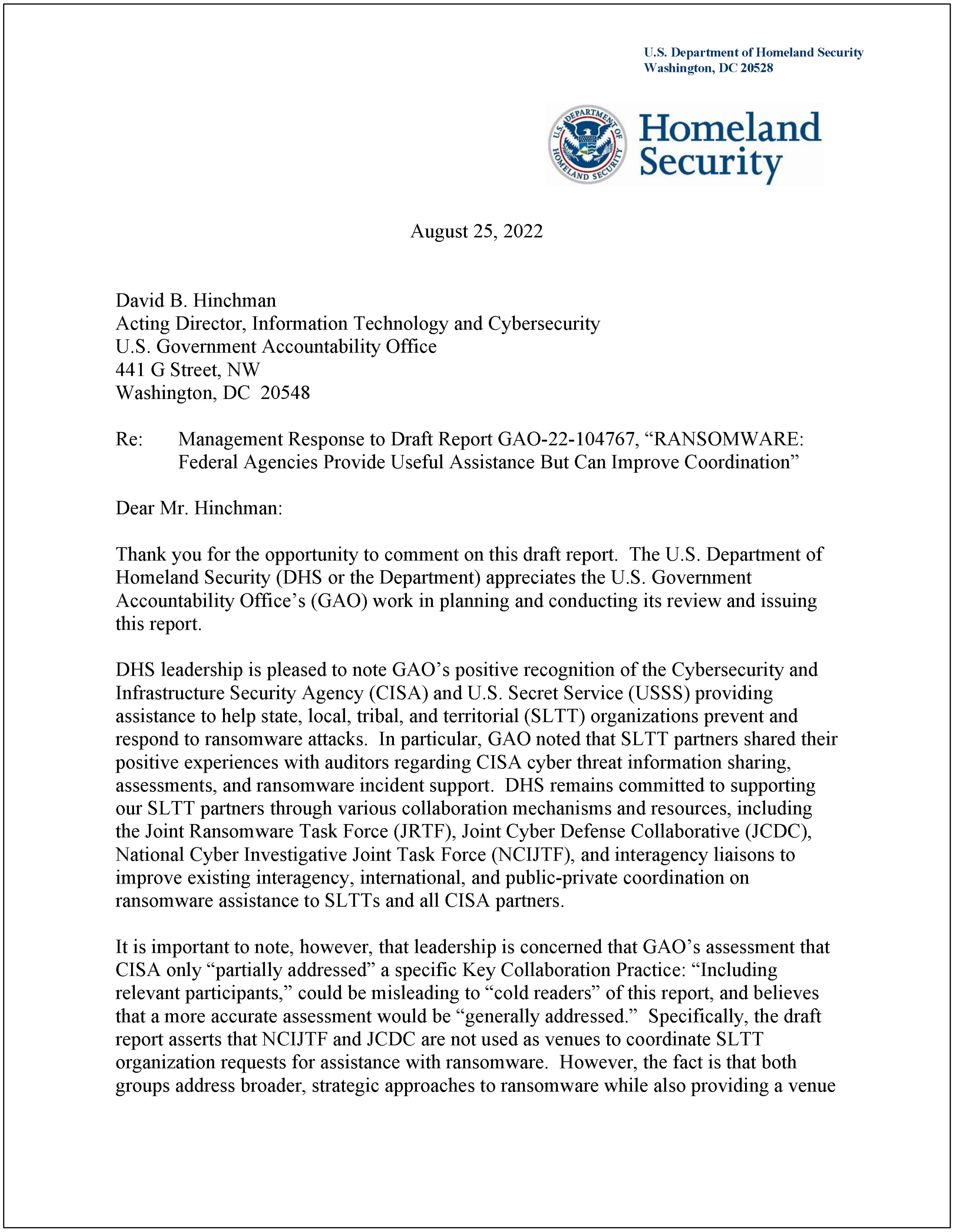
If you or your staff have any questions about this report, please contact me at (214) 777-5719, or HinchmanD@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix II.

Sincerely yours,

David B Hinchman

David B. Hinchman
Acting Director, Information Technology and Cybersecurity

Appendix I: Comments from the Department of Homeland Security



U.S. Department of Homeland Security
Washington, DC 20528

August 25, 2022

David B. Hinchman
Acting Director, Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

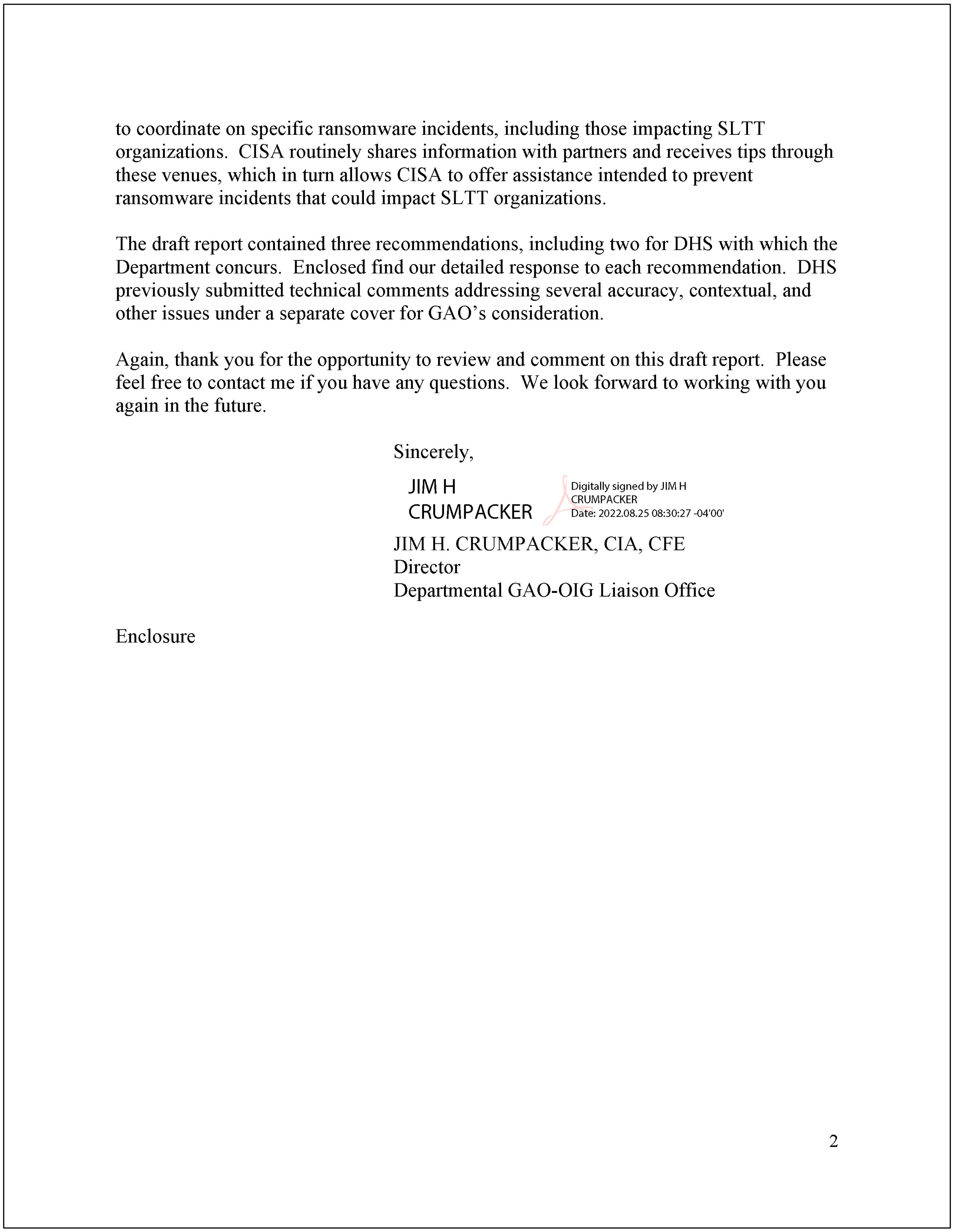
Re: Management Response to Draft Report GAO-22-104767, "RANSOMWARE: Federal Agencies Provide Useful Assistance But Can Improve Coordination"

Dear Mr. Hinchman:

Thank you for the opportunity to comment on this draft report. The U.S. Department of Homeland Security (DHS or the Department) appreciates the U.S. Government Accountability Office's (GAO) work in planning and conducting its review and issuing this report.

DHS leadership is pleased to note GAO's positive recognition of the Cybersecurity and Infrastructure Security Agency (CISA) and U.S. Secret Service (USSS) providing assistance to help state, local, tribal, and territorial (SLTT) organizations prevent and respond to ransomware attacks. In particular, GAO noted that SLTT partners shared their positive experiences with auditors regarding CISA cyber threat information sharing, assessments, and ransomware incident support. DHS remains committed to supporting our SLTT partners through various collaboration mechanisms and resources, including the Joint Ransomware Task Force (JRTF), Joint Cyber Defense Collaborative (JCDC), National Cyber Investigative Joint Task Force (NCIJTF), and interagency liaisons to improve existing interagency, international, and public-private coordination on ransomware assistance to SLTTs and all CISA partners.

It is important to note, however, that leadership is concerned that GAO's assessment that CISA only "partially addressed" a specific Key Collaboration Practice: "Including relevant participants," could be misleading to "cold readers" of this report, and believes that a more accurate assessment would be "generally addressed." Specifically, the draft report asserts that NCIJTF and JCDC are not used as venues to coordinate SLTT organization requests for assistance with ransomware. However, the fact is that both groups address broader, strategic approaches to ransomware while also providing a venue



to coordinate on specific ransomware incidents, including those impacting SLTT organizations. CISA routinely shares information with partners and receives tips through these venues, which in turn allows CISA to offer assistance intended to prevent ransomware incidents that could impact SLTT organizations.

The draft report contained three recommendations, including two for DHS with which the Department concurs. Enclosed find our detailed response to each recommendation. DHS previously submitted technical comments addressing several accuracy, contextual, and other issues under a separate cover for GAO's consideration.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

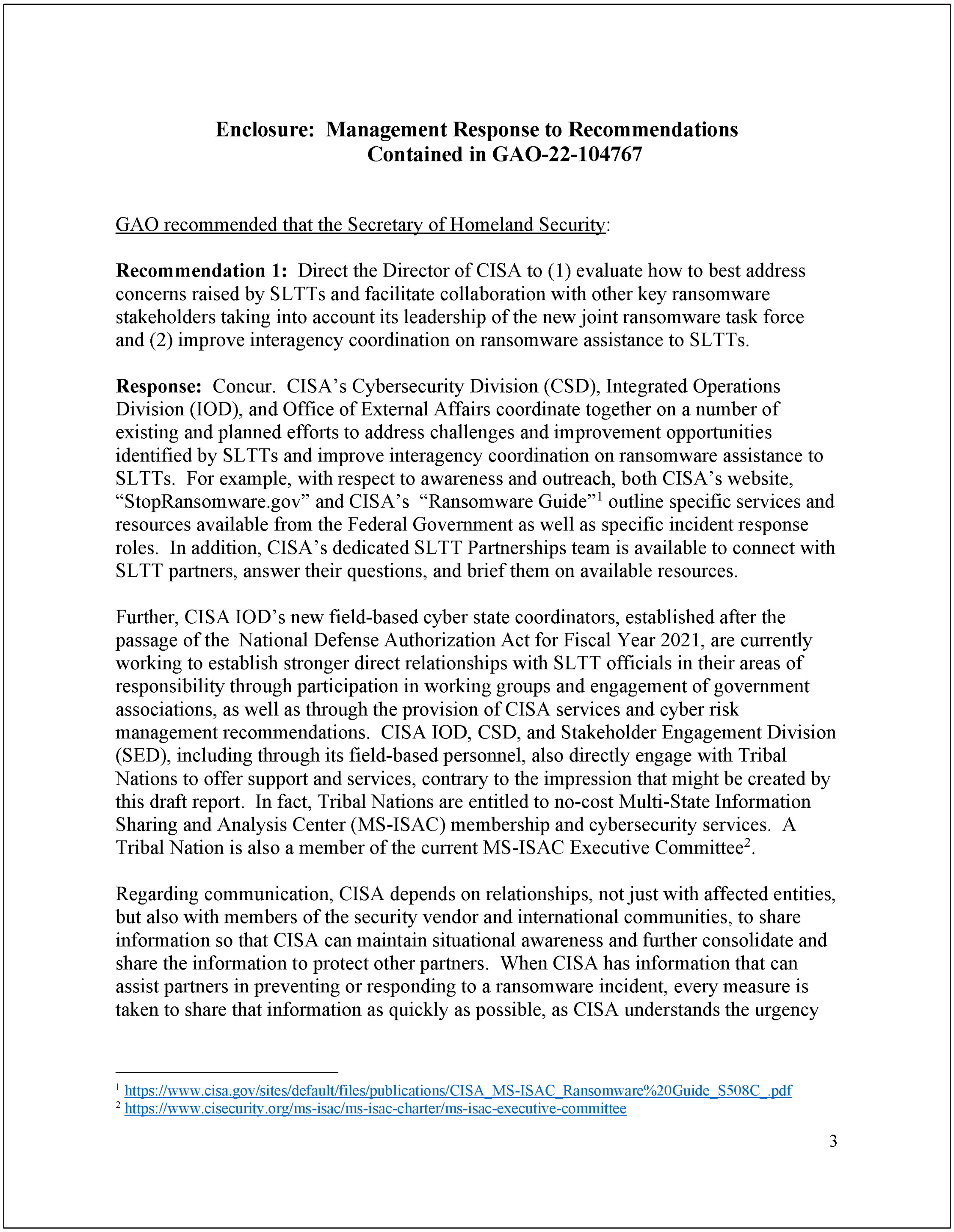
Sincerely,

JIM H
CRUMPACKER

Digitally signed by JIM H
CRUMPACKER
Date: 2022.08.25 08:30:27 -04'00'

JIM H. CRUMPACKER, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

Enclosure



Enclosure: Management Response to Recommendations Contained in GAO-22-104767

GAO recommended that the Secretary of Homeland Security:

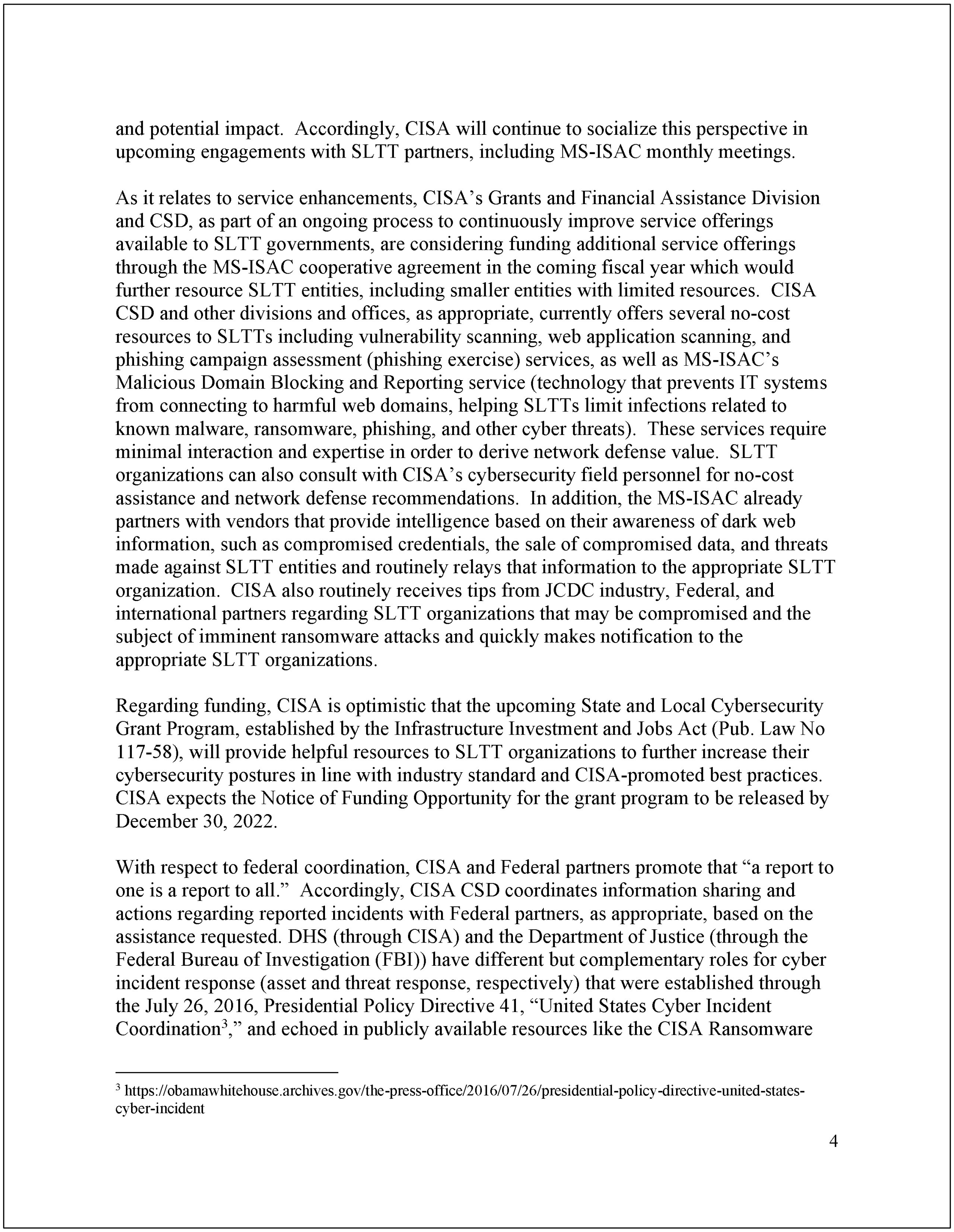
Recommendation 1: Direct the Director of CISA to (1) evaluate how to best address concerns raised by SLTTs and facilitate collaboration with other key ransomware stakeholders taking into account its leadership of the new joint ransomware task force and (2) improve interagency coordination on ransomware assistance to SLTTs.

Response: Concur. CISA's Cybersecurity Division (CSD), Integrated Operations Division (IOD), and Office of External Affairs coordinate together on a number of existing and planned efforts to address challenges and improvement opportunities identified by SLTTs and improve interagency coordination on ransomware assistance to SLTTs. For example, with respect to awareness and outreach, both CISA's website, "StopRansomware.gov" and CISA's "Ransomware Guide"[1] outline specific services and resources available from the Federal Government as well as specific incident response roles. In addition, CISA's dedicated SLTT Partnerships team is available to connect with SLTT partners, answer their questions, and brief them on available resources.

Further, CISA IOD's new field-based cyber state coordinators, established after the passage of the National Defense Authorization Act for Fiscal Year 2021, are currently working to establish stronger direct relationships with SLTT officials in their areas of responsibility through participation in working groups and engagement of government associations, as well as through the provision of CISA services and cyber risk management recommendations. CISA IOD, CSD, and Stakeholder Engagement Division (SED), including through its field-based personnel, also directly engage with Tribal Nations to offer support and services, contrary to the impression that might be created by this draft report. In fact, Tribal Nations are entitled to no-cost Multi-State Information Sharing and Analysis Center (MS-ISAC) membership and cybersecurity services. A Tribal Nation is also a member of the current MS-ISAC Executive Committee[2].

Regarding communication, CISA depends on relationships, not just with affected entities, but also with members of the security vendor and international communities, to share information so that CISA can maintain situational awareness and further consolidate and share the information to protect other partners. When CISA has information that can assist partners in preventing or responding to a ransomware incident, every measure is taken to share that information as quickly as possible, as CISA understands the urgency

[1] https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf
[2] https://www.cisecurity.org/ms-isac/ms-isac-charter/ms-isac-executive-committee



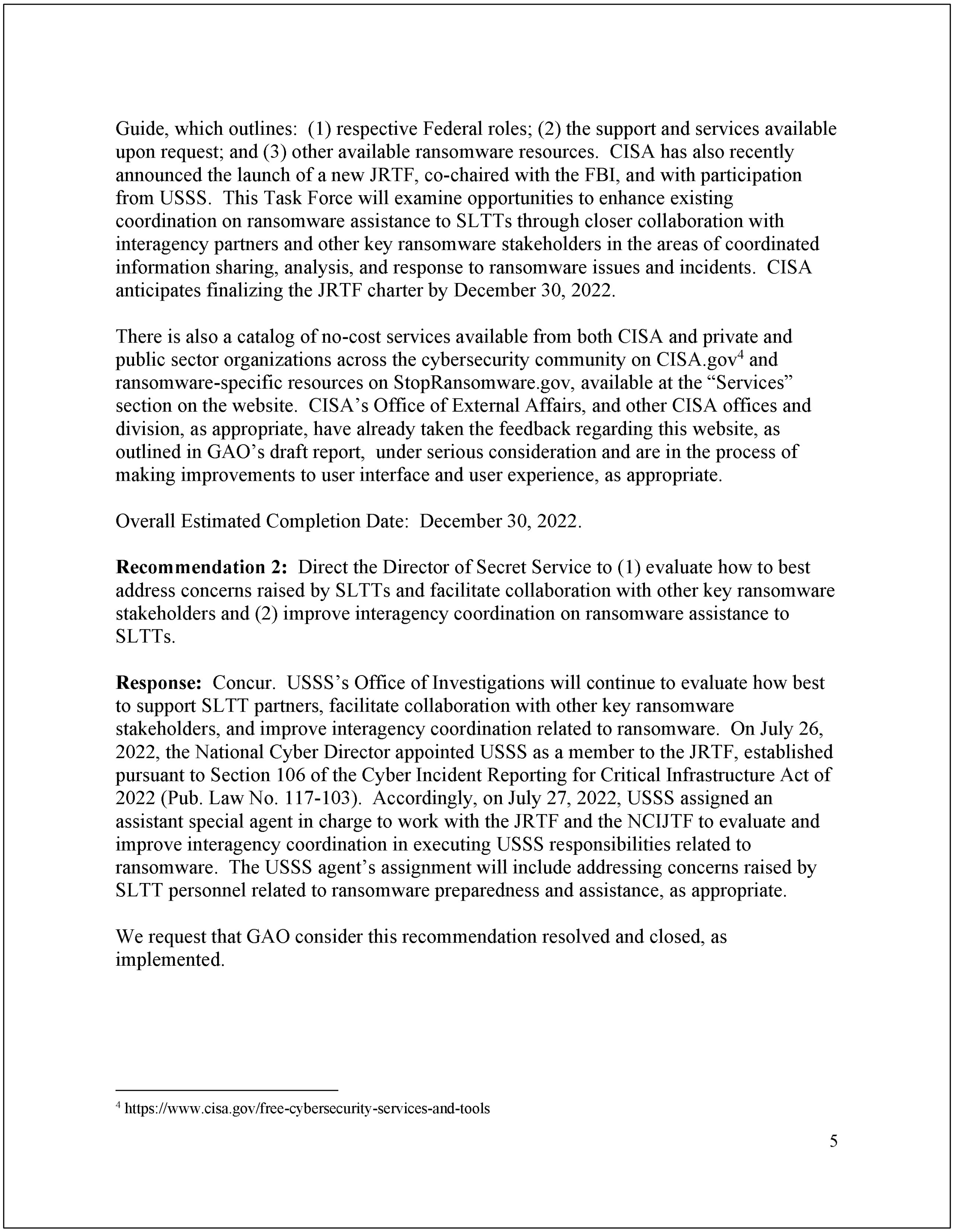
and potential impact. Accordingly, CISA will continue to socialize this perspective in upcoming engagements with SLTT partners, including MS-ISAC monthly meetings.

As it relates to service enhancements, CISA's Grants and Financial Assistance Division and CSD, as part of an ongoing process to continuously improve service offerings available to SLTT governments, are considering funding additional service offerings through the MS-ISAC cooperative agreement in the coming fiscal year which would further resource SLTT entities, including smaller entities with limited resources. CISA CSD and other divisions and offices, as appropriate, currently offers several no-cost resources to SLTTs including vulnerability scanning, web application scanning, and phishing campaign assessment (phishing exercise) services, as well as MS-ISAC's Malicious Domain Blocking and Reporting service (technology that prevents IT systems from connecting to harmful web domains, helping SLTTs limit infections related to known malware, ransomware, phishing, and other cyber threats). These services require minimal interaction and expertise in order to derive network defense value. SLTT organizations can also consult with CISA's cybersecurity field personnel for no-cost assistance and network defense recommendations. In addition, the MS-ISAC already partners with vendors that provide intelligence based on their awareness of dark web information, such as compromised credentials, the sale of compromised data, and threats made against SLTT entities and routinely relays that information to the appropriate SLTT organization. CISA also routinely receives tips from JCDC industry, Federal, and international partners regarding SLTT organizations that may be compromised and the subject of imminent ransomware attacks and quickly makes notification to the appropriate SLTT organizations.

Regarding funding, CISA is optimistic that the upcoming State and Local Cybersecurity Grant Program, established by the Infrastructure Investment and Jobs Act (Pub. Law No 117-58), will provide helpful resources to SLTT organizations to further increase their cybersecurity postures in line with industry standard and CISA-promoted best practices. CISA expects the Notice of Funding Opportunity for the grant program to be released by December 30, 2022.

With respect to federal coordination, CISA and Federal partners promote that "a report to one is a report to all." Accordingly, CISA CSD coordinates information sharing and actions regarding reported incidents with Federal partners, as appropriate, based on the assistance requested. DHS (through CISA) and the Department of Justice (through the Federal Bureau of Investigation (FBI)) have different but complementary roles for cyber incident response (asset and threat response, respectively) that were established through the July 26, 2016, Presidential Policy Directive 41, "United States Cyber Incident Coordination[3]," and echoed in publicly available resources like the CISA Ransomware

[3] https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident



Guide, which outlines: (1) respective Federal roles; (2) the support and services available upon request; and (3) other available ransomware resources. CISA has also recently announced the launch of a new JRTF, co-chaired with the FBI, and with participation from USSS. This Task Force will examine opportunities to enhance existing coordination on ransomware assistance to SLTTs through closer collaboration with interagency partners and other key ransomware stakeholders in the areas of coordinated information sharing, analysis, and response to ransomware issues and incidents. CISA anticipates finalizing the JRTF charter by December 30, 2022.

There is also a catalog of no-cost services available from both CISA and private and public sector organizations across the cybersecurity community on CISA.gov[4] and ransomware-specific resources on StopRansomware.gov, available at the “Services” section on the website. CISA’s Office of External Affairs, and other CISA offices and division, as appropriate, have already taken the feedback regarding this website, as outlined in GAO’s draft report, under serious consideration and are in the process of making improvements to user interface and user experience, as appropriate.

Overall Estimated Completion Date: December 30, 2022.

Recommendation 2: Direct the Director of Secret Service to (1) evaluate how to best address concerns raised by SLTTs and facilitate collaboration with other key ransomware stakeholders and (2) improve interagency coordination on ransomware assistance to SLTTs.

Response: Concur. USSS’s Office of Investigations will continue to evaluate how best to support SLTT partners, facilitate collaboration with other key ransomware stakeholders, and improve interagency coordination related to ransomware. On July 26, 2022, the National Cyber Director appointed USSS as a member to the JRTF, established pursuant to Section 106 of the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (Pub. Law No. 117-103). Accordingly, on July 27, 2022, USSS assigned an assistant special agent in charge to work with the JRTF and the NCIJTF to evaluate and improve interagency coordination in executing USSS responsibilities related to ransomware. The USSS agent’s assignment will include addressing concerns raised by SLTT personnel related to ransomware preparedness and assistance, as appropriate.

We request that GAO consider this recommendation resolved and closed, as implemented.

[4] https://www.cisa.gov/free-cybersecurity-services-and-tools

Appendix II: GAO Contacts and Staff Acknowledgments

GAO Contact

David B. Hinchman, (214) 777-5719, or HinchmanD@gao.gov

Staff Acknowledgments

In addition to the contacts listed above, the following staff made significant contributions to this report: Josh Leiling (Assistant Director), Torrey Hardee (Analyst in Charge), Chris Businsky, Quade Bywater, Joseph P. Cruz, Vijay D’Souza, Rebecca Eyler, Andrea Harvey, Franklin Jackson, Heather Ko, Cecil Murfree, Ashley Paw, Walter Vance, and Sarah Veale.

(104767)

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or
TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/about/what-gao-does/fraudnet

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

Stephen J. Sanford, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548

Please Print on Recycled Paper.