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

September 2022

RANSOMWARE

Federal Agencies Provide Useful Assistance but Can Improve Collaboration

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.

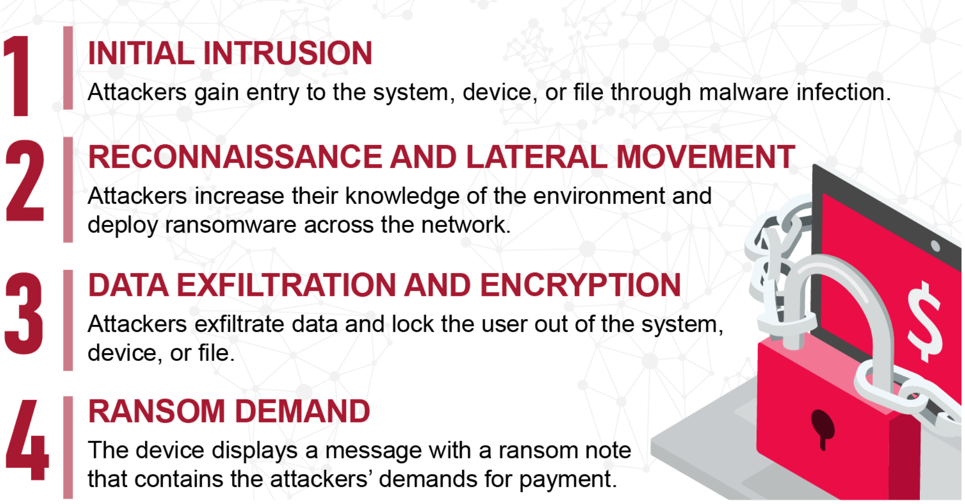
GAO reviewed agency documentation from eight federal agencies to identify efforts to help state, local, tribal and territorial governments address ransomware threats. Documents reviewed included agency service catalogs, ransomware guidance, and agency websites. GAO supplemented these reviews with interviews 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.

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.