

WTA RURAL BROADBAND: ADVANCED PERSISTENT THREATS — AN OVERVIEW

Richard (Dick) Tenney

Senior Advisor, Cyber

Emergency Communications Division

Cybersecurity and Infrastructure Security Agency (CISA)



Cyber Threat Overview

Threat Actors Targeting the Sector:

- Advanced Persistent Threats (APTs).
- Nation-states.
- Ransomware groups.
- Hackers.



Intent and Motive:

- Leverage compromised infrastructure to conduct malicious cyber campaigns.
- Gain access to sensitive customer information.
- Compromise infrastructure to deny access to customers.
- Deploy ransomware for financial gain.

Common Tactics, Techniques, and Procedures (TTPs)

Distributed Denial of Service (DDoS) | Spearphishing | Ransomware



What is Cybersecurity Risk?

Cyber Risk: Likelihood any specific threat will exploit a specific vulnerability that causes harm as a result of unauthorized disclosure, modification, or destruction/loss of information or system availability.

Threat

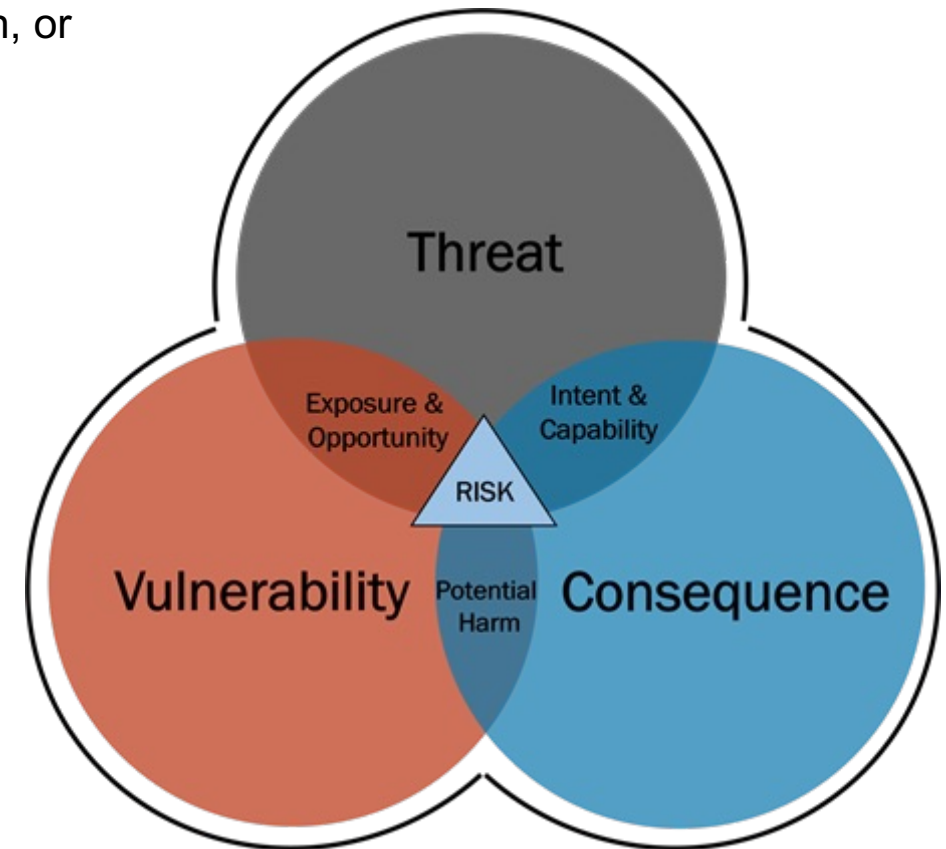
- People, programs, hardware, or systems with intent, capability, and opportunity to exploit vulnerabilities.

Vulnerability





- Weakness in the information (IT) or operational (OT) technology infrastructure or other aspect of an organization.

Consequence

- Effect of an event, incident, or occurrence.



Nation-State Affiliated APT Groups

Designator	Examples of Malware	
APT 41 – China	<ul style="list-style-type: none"> • Red Apollo • MenuPass • Stone Panda 	
APT 40 – China	<ul style="list-style-type: none"> • MUDCARP • Kryptonite Panda • Gadolinium • Leviathan 	
APT 28 – Russia	<ul style="list-style-type: none"> • Pawn Storm • Fancy Bear • Strontium 	
APT 29 – Russia	<ul style="list-style-type: none"> • Cozy Bear • Nobelium • Dark Halo • NobleBaron 	
APT 35 – Iran	<ul style="list-style-type: none"> • Charming Kitten • Cobalt Illusion • Phosphorous • Newscaster • TA453 	
APT 38 – North Korea	<ul style="list-style-type: none"> • Lazarus • Reaper 	



Sector Cyber Hygiene

Communications and IT Sector entities operating with internet-accessible products, applications, and software that possess vulnerabilities are actively exploited by threat actors to compromise public and private entities.

- This analysis is derived from the CISA Cyber Hygiene (CyHy) Vulnerability Scanning (VS) and Web Application Scanning (WAS) services as of Feb 2023.
 - 296 Sector entities scanned via CyHy VS
 - Communications: 52
 - IT: 244
 - 149 Sector entities scanned via WAS
 - Communications: 19
 - IT: 130



CISA offers free services to enable entities to reduce their internet accessible attack surface.
Email vulnerability@cisa.dhs.gov for more information and to sign up.



Known Exploited Vulnerabilities (KEV)

CISA maintains authoritative source of Known Exploited Vulnerabilities (KEVs), which identifies subset of Common Vulnerabilities and Exposures (CVEs) that are actively used to compromise systems. Organizations should use the KEV catalog as an input to their vulnerability management and prioritization framework.

For more information, visit: cisa.gov/known-exploited-vulnerabilities/

As of February 1st, 2023, there were 37 distinct entities (IT and Communications) running software associated with Apache, Cisco, Microsoft, MikroTik, OpenSSL, PHP, PrimeTek, and Serv-U, that exposed KEVs.

Includes continued exposure of **CVE-2021-44228*** that is associated with Log4j, a widespread exploitation of a critical remote code execution that has historically enabled threat actors to gain access, escalate privileges, and maintain a foothold on entity networks. CISA urges entities to remediate KEVs as soon as possible after identification to decrease risk of compromise.

**This CVE was also seen via industry threat data reporting as being ranked with the highest observed detection within customer environments. These detections included malicious exploitation and non-malicious activities (i.e., scanning)*

Vendor	CVE	Base Score
Apache	CVE-2017-12617	8.1 High
	CVE-2020-1938	9.8 Critical
	CVE-2021-40438	9.0 Critical
	CVE-2021-44228*	10.0 Critical
Cisco	CVE-2020-3452	7.5 High
	CVE-2020-3580	6.1 Medium
Microsoft	CVE-2020-1350	10.0 Critical
MikroTik	CVE-2018-7445	9.8 Critical
OpenSSL	CVE-2014-0160	7.5 High
PHP	CVE-2012-1823	N/A
	CVE-2019-11043	9.8 Critical
PrimeTek	CVE-2017-1000486	9.8 Critical
Serv-U	CVE-2021-35211	10.0 Critical
	CVE-2021-35247	5.3 Medium



Vulnerabilities of Concern

MSP	Attack Details
Cott Systems	<ul style="list-style-type: none">• Ransomware attack in December 2022, affecting at least 17 county governments in 6 states, primarily County Clerk’s offices
RackSpace	<ul style="list-style-type: none">• Ransomware attack on Hosted Exchange business caused Email outages experienced by thousands of its customers in December 2022• Attributed to a financially-motivated “known ransomware group”
SolarWinds	<ul style="list-style-type: none">• One of the most sophisticated and large-scale cyber operations ever identified.• An intelligence gathering effort discovered in December 2020, attributed to an actor that is likely Russian in origin
TSM Consulting	<ul style="list-style-type: none">• Impacted at least 22 Texas municipal IT systems in August 2019• Attributed to Russian REvil hacker gang
Kaseya	<ul style="list-style-type: none">• Digital supply chain attack effecting over 1,500 Kaseya customers in July 2019• Also attributed to REvil



TSM Consulting, Texas: Use Case

Case 3:21-cr-00093 Document 1 Filed 08/24/21 Page 1 of 23 PageID 5

ORIGINAL **SEALED**

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

CLERK OF DISTRICT COURT
NORTHERN DISTRICT OF TX
FILED
2021 AUG 24 PM 5: 03
DEPUTY CLERK

UNITED STATES OF AMERICA
V.
Yevgeniy Igorevich Polyanin (01)
a/k/a Evgeniy Igorevich Polyanin
a/k/a Evgeniy Polyanin
a/k/a LR4D4
a/k/a Damnating
a/k/a Damn2life
a/k/a Noolleds
a/k/a Antanpire
a/k/a Affiliate 23

CRIMINAL NO.
FILED UNDER SEAL
8-21CR0393-B

INDICTMENT

The Grand Jury charges:
At all times material to this indictment:
General Allegations

1. "Malware" was a malicious software program designed to disrupt computer operations, gather sensitive information, gain access to private computer systems, and perform other unauthorized actions on computer systems. Common examples of malware included viruses, ransomware, worms, keyloggers, and spyware.
2. "Ransomware" was a type of malware that infected a computer and encrypted some or all of the data on the computer. Distributors of ransomware typically extorted the user of the encrypted computer by demanding that the user pay a ransom in order to decrypt and recover the data on the computer.

Indictment - Page 1

WANTED BY THE FBI

YEVGYENIY IGORYEVICH POLYANIN

Conspiracy to Commit Fraud and Related Activity in Connection with Computers; Intentional Damage to a Protected Computer; Conspiracy to Commit Money Laundering



DESCRIPTION

Aliases: Yevgyenyiy Polyanin, Yevgeniy Polyanin, Yevgeniy Igorevich Polyanin, Evgeniy Igorevich Polyanin, Evgeniy Polyanin, Evgeniy Igorevich Polyanin, "54-481"

Date(s) of Birth Used: March 4, 1993 Place of Birth: Russia

Sex: Male Race: White

Nationality: Russian

REMARKS

Polyanin is believed to be in Russia, possibly in Samara, and is one of many Sodnokits/REvil ransomware affiliates.

CAUTION

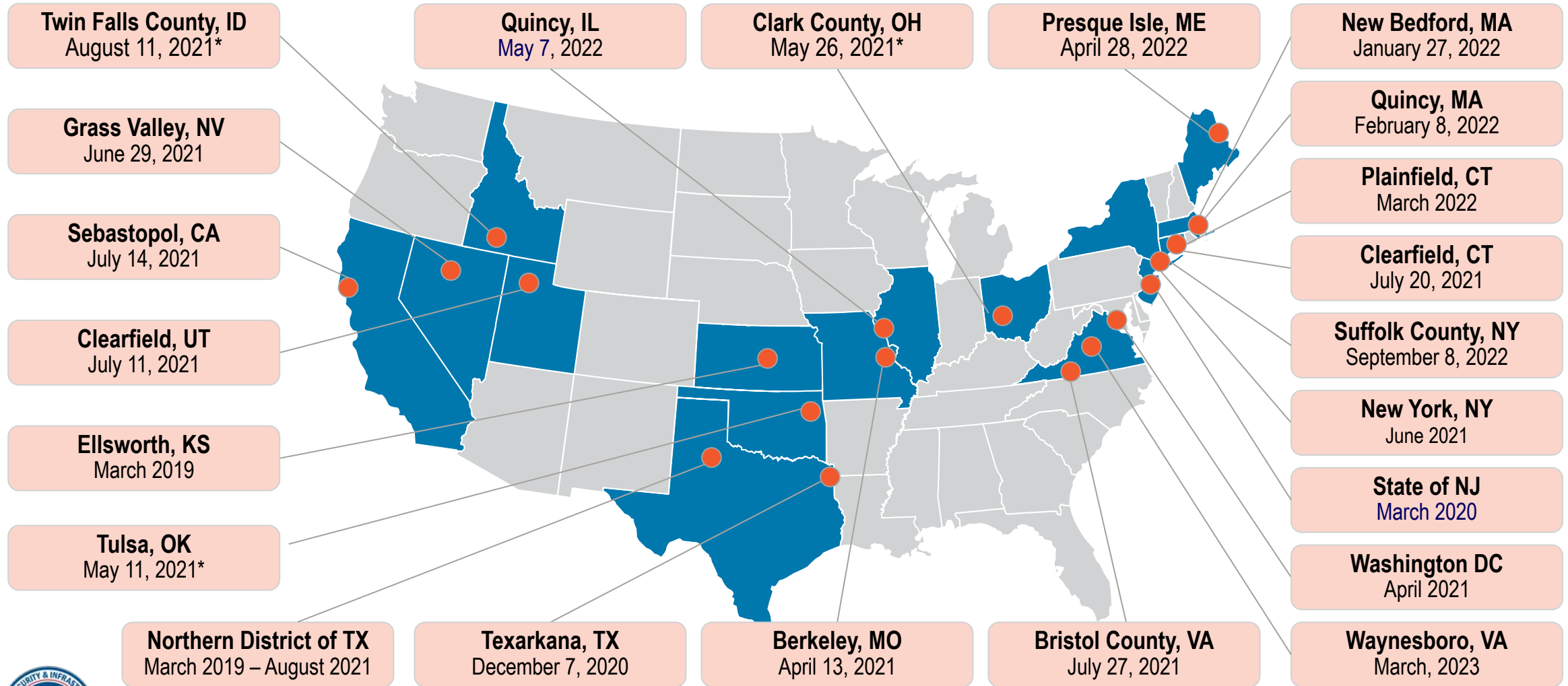
Yevgeniy Igorevich Polyanin is wanted for his alleged involvement in ransomware attacks and money laundering activities. It is alleged that, through the use and deployment of Sodnokits and REvil ransomware, Polyanin left electronic notes in the form of a text file on victims' computers. The notes included web addresses for the victims to visit and have their files decrypted. Upon visiting these web addresses, victims were given the ransom amount demanded and provided a virtual currency address to use to pay the ransom. If a victim paid the ransom amount, Polyanin provided the decryption key, and the victims then were able to access their files. If a victim did not pay the ransom, Polyanin typically posted the victims' exfiltrated data or claimed he sold the exfiltrated data to third parties. Polyanin has been charged in an indictment filed in the United States District Court for the Northern District of Texas, Dallas, Texas, with conspiracy to commit fraud and related activity in connection with computers, substantive counts of intentional damage to protected computers, and conspiracy to commit money laundering.

If you have any information concerning this person, please contact your local FBI office or the nearest American Embassy or Consulate.

Field Office: Dallas



Examples of Public Safety Attacks



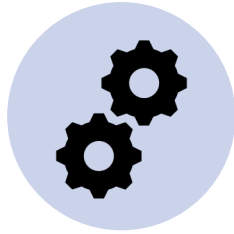
*Open source information; Managed service provider attack

CISA GETS / WPS / TSP

- **Wireless Priority Service (WPS), Government Emergency Telecommunications Service (GETS), and Telecommunications Service Priority (TSP):**
 - Provided by CISA to ensure essential organizations/personnel have access to priority telecommunications and restoration services.
 - Essential organizations within all levels of government, private sector, and NGOs
- **CISA Priority Telecommunications Service Center determines eligibility and assigns categories:**
 - Executive personnel and policy makers
 - Disaster response, military command and control personnel
 - Public health, public safety and law enforcement personnel
 - Public services/utilities, public welfare, and critical infrastructure protection personnel
 - Disaster recovery personnel
- **Eligibility/Enrollment**
 - Contact the CISA Priority Telecommunications Service Center at:
 - (866) 627-2255
 - Email ecd@cisa.dhs.gov or visit cisa.gov/pts.



Actions to Reduce Cyber Risk



Manage and Secure Assets

- Implement network segmentation to separate assets based on sensitivity and function. ([CISA CPG 8.1](#))
- Reduce attack surface with properly configured firewalls and strong encryption mechanisms. ([CISA CPG 3.3 and 8.1](#))
- Maintain comprehensive documentation of assets, configurations, supporting business functions and current version information. ([CISA CPG 2.1, 2.3, and 2.5](#))
- Prohibit connection of unauthorized media and hardware. ([CISA CPG 2.4](#))
- Monitor access and security event logs. ([CISA CPG 3.1](#))



Minimize Vulnerable Service Exposure

- Minimize network exposure to only those services required by business need. ([CISA CPG 5.4 and 5.5](#))
- Ensure security policy prohibits exposure of services that are inherently insecure. ([CISA CPG 2.1, 5.4, and 5.5](#))
- If after careful consideration, business operations require exposure of sensitive services.
 - Require use of more secure alternatives
 - Follow vendor guidance to configure secure encryption protocols ([CISA CPG 3.3](#))
 - For remote access, implement MFA and harden VPN solutions ([CISA CPG 1.3](#))



Implement Robust Vulnerability Management

- Prioritize resources towards patching assets which support critical business functions. ([CISA CPG 5.1](#))
- Implement policy to handle out-of-cycle patching for potentially critical vulnerabilities, such as KEVs. ([CISA CPG 5.1](#))
- Develop and implement a performance mechanism to track adherence to established patch deadlines and inform resourcing requirements. ([CISA CPG 2.3](#))



Visit CISA's [Cross-Sector Cybersecurity Performance Goals](#) for more information on the CPGs, including additional recommended baseline protections.

CISA Services Reduce Cyber Risk

Newly enrolled entities typically see drastic decreases in exposed vulnerabilities within their first three months of scanning.

CISA offers **free** cybersecurity services to IT and Communications entities:

- **Vulnerability Scanning:** Entities can identify vulnerabilities and enable their remediation through persistent scanning of internet-accessible systems for weaknesses, configuration errors, and suboptimal security practices.

Email vulnerability@cisa.dhs.gov for more information and to sign up.



Cryptocurrency

US Senate Committee on Homeland Security...

- In 2020, at least \$692 million in cryptocurrency extorted as part of ransomware attacks
- Lack of comprehensive data on the amount of ransomware attacks and use of cryptocurrency as ransom payments in these attacks
- Bitcoin — primary currency for ransom payment
 - Cryptocurrency enables criminals to extort huge sums from victims across diverse sectors with incredible speed
 - Increasingly, cybercriminals demanding payment in Monero and Ethereum, likely due to the heightened anonymity



Cyber Insurance

- Cyber Insurance — coverage that can protect a business from losses caused by cyber attacks
- Demand and cost of cyber insurance increasing rapidly
- Market volatility leading to companies choosing to not cover various types of cyber attacks and charging high premiums for various industries
- A Government Accountability Office report was released in June 2022 recommending Federal Insurance Office and CISA conduct a joint assessment



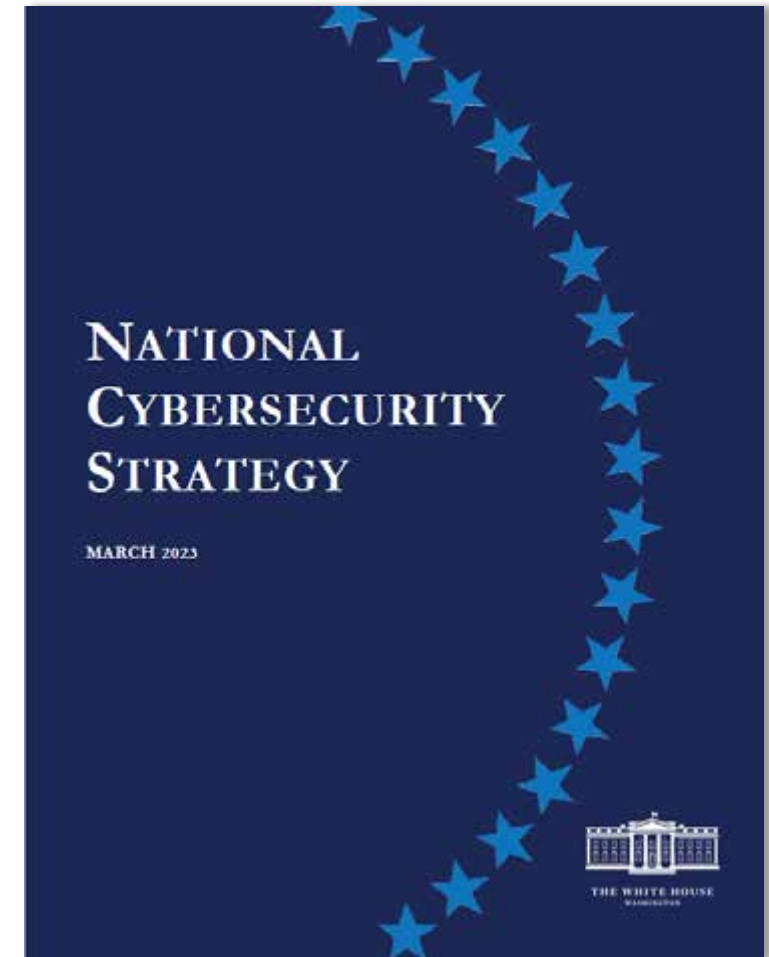
National Cybersecurity Strategy

The White House released the National Cybersecurity Strategy in March 2023. There are two main focuses of the strategy:

1. Rebalance the responsibility to defend cyberspace
2. Realign incentives to favor long-term investments

WHAT IS CISA'S ROLE IN THE STRATEGY?

- Remove Barriers to Threat Information Sharing Between Government and the Private Sector
- Modernizing and Implementing Stronger Cybersecurity Standards across the Federal Government
- Improve Software Supply Chain Security
- Establish a Cyber Safety Review Board
- Create Standardized Playbook for Responding to Cybersecurity Vulnerabilities and Incidents
- Improve Detection of Cybersecurity Incidents on Federal Government Networks
- Improve Investigative and Remediation Capabilities



CIR CIA

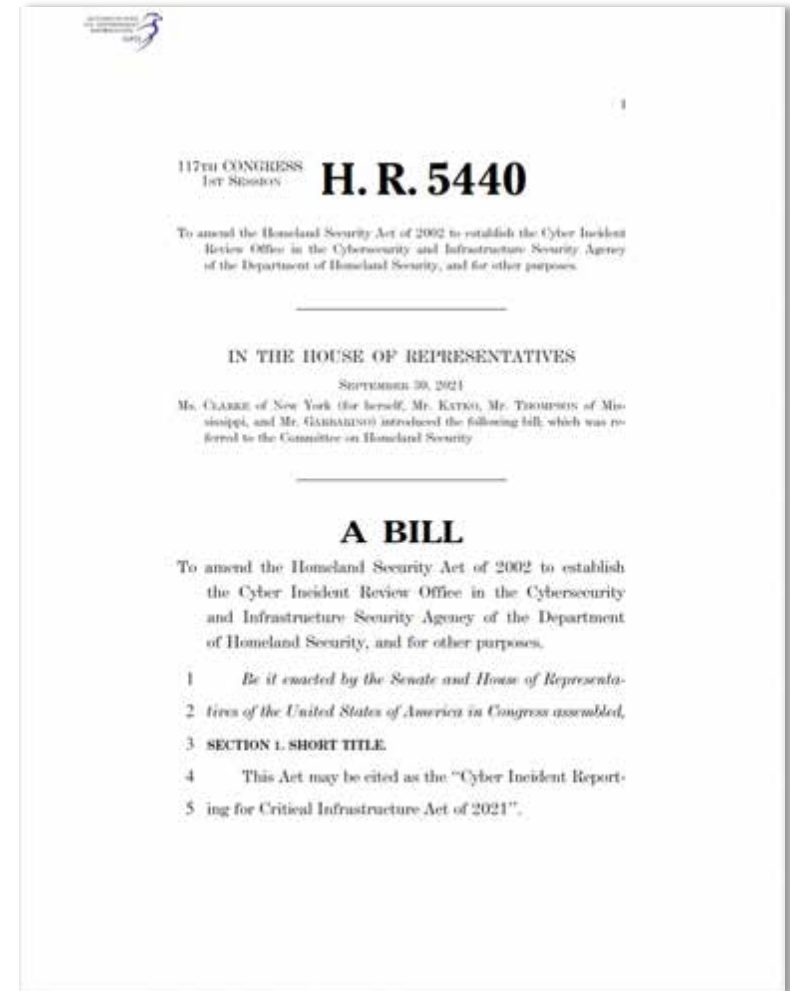
WHAT IS CIR CIA?

The Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIR CIA) was signed by President Biden in March of 2022.

In accordance with CIR CIA, CISA will now undertake a rulemaking process to implement the statutory requirements. In the interim, CISA continues to encourage our stakeholders to voluntarily share information about cyber-related events that could help mitigate current or emerging cybersecurity threats to critical infrastructure.

WHAT TYPES OF ACTIVITY SHOULD YOU SHARE WITH CISA

- Unauthorized access to your system
- Denial of Service (DOS) attacks that last more than 12 hours
- Malicious code on your systems, including variants if known
- Targeted and repeated scans against services on your systems
- Repeated attempts to gain unauthorized access to your system
- Email or mobile messages associated with phishing attempts or successes
- Ransomware against Critical Infrastructure, include variant and ransom details if known



State and Local Cybersecurity Grant Program

- The Infrastructure Investment and Jobs Act amended the Homeland Security Act and appropriated **\$1 Billion for SLTT cybersecurity grants over 4 years** (Fiscal Year 2022 – 2025)
 - First-of-its-kind grant program for SLTT cybersecurity, with CISA and FEMA jointly managing
- **Eligibility:**
 - Eligible entities are states and territories' State Administrative Agency (SAA) with subawards to local entities
 - Multi-entity grants can be made to groups of eligible entities with additional incentives
- **Funding:**
 - Formula-based with states/territories receiving a baseline allocation plus population-based allocation
 - 80% of funds pass through to local entities
 - 25% of total state/territory allocation must go to rural communities
 - Increasing state, local, tribal, and territorial (SLTT) cost share requirement over time



Program Status and Next Steps

- **Program Status:**

- **Applications:** 54 of the 56 eligible states and territories applied.
- **Cybersecurity Plans/Planning Committees:** Within those 54 applications, 13 Cybersecurity Plans have been submitted, 11 have been approved and 2 are currently under review.
 - FEMA is conducting detailed budget reviews for the approved plans and will release fundings holds as completed.
- **Overall Award Picture:** FEMA completed all Fiscal Year 2022 State and Local Cybersecurity Grant Program award notifications before December 31, 2022.

- **Next Steps:**

- **Cybersecurity Plans:** Entities that have not yet completed a Cybersecurity Plan or need additional assistance should contact CISA Regional Staff.
 - Cybersecurity Plans must be submitted to CISA and FEMA by September 30, 2023.
- **FY23 NOFO:** CISA and FEMA anticipate a release date of mid-2023 with a process similar to FY22.





For more information:
www.cisa.gov

Questions?
Email: Richard.Tenney@cisa.dhs.gov
Phone: 202-422-2668



BACKUP SLIDES



REMCDP/O-RAP

Purpose

Through demonstration projects with up to two public and state-controlled institutions of higher education, REMCDP's goal is to **examine** communications barriers and identify solutions that enhance existing emergency communications infrastructure to improve the delivery of rural medical care and address NECP implementation gaps.

Dedicated assistance to local and tribal rural communities to improve emergency medical communications.



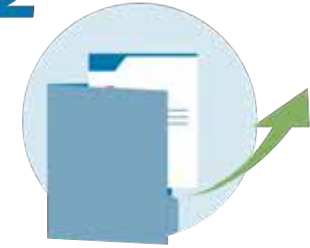
1



Site Survey

Site visit to understand gaps and needs

2



Policies, Plans, Procedures

Address a specific need selected from site survey

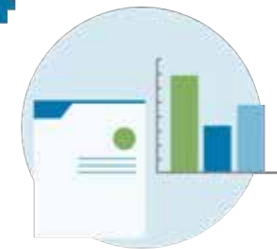
3



Training

Develop training related to the policy, plan, or procedure

4



Exercise

Test and evaluate the policy, plan, or procedure and training

CISA Emergency Communications Division

April 25, 2023

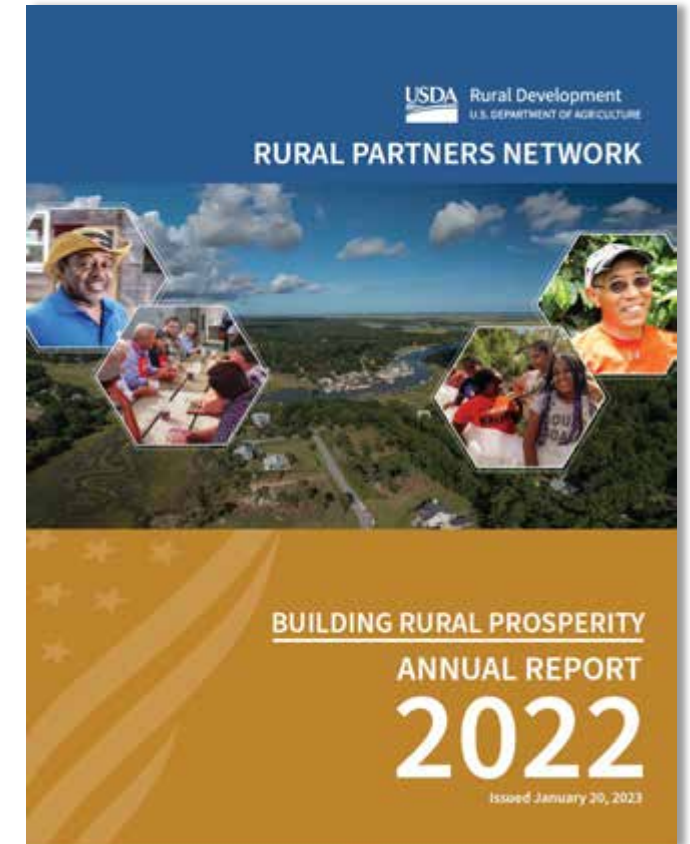
Nation-State Affiliated APT Groups

Designator	Examples of Malware	Targets and Victims
APT 41 China	<ul style="list-style-type: none"> Red Apollo MenuPass Stone Panda 	<ul style="list-style-type: none"> More than 45 companies in at least a dozen states, managed service providers, and U.S. government agencies 8 states' networks attacked, early 2022 Downstream businesses in at least 12 countries \$20 million in US Covid relief benefits, including small business administration loans and unemployment insurance funds in over a dozen states
APT 40 China	<ul style="list-style-type: none"> MUDCARP Kryptonite Panda Gadolinium Leviathan 	<ul style="list-style-type: none"> Trade secrets, intellectual property, and other high value information: aviation, defense, education, government, health care, biopharmaceutical, maritime transport US COVID Relief Funds
APT 28 Russia	<ul style="list-style-type: none"> Pawn Storm Fancy Bear Strontium 	<ul style="list-style-type: none"> Democratic National Convention 2016 Presidential Election ViaSat Satellite Network
APT 29 Russia	<ul style="list-style-type: none"> Cozy Bear Nobelium Dark Halo NobleBaron 	<ul style="list-style-type: none"> Government – Phishing attacks on diplomats Technology - SolarWinds Telecommunications
APT 35 Iran	<ul style="list-style-type: none"> Charming Kitten Cobalt Illusion Phosphorous Newscaster TA453 	<ul style="list-style-type: none"> Groups in political opposition to Iran's Islamic Revolutionary Guard Corps Academic and educational institutions and individuals in the U.S, France, and the Middle East Extensive use of Log4J and Microsoft Exchange Server vulnerabilities
APT 38 North Korea	<ul style="list-style-type: none"> Lazarus Reaper 	<ul style="list-style-type: none"> 2022 Ronin Bridge - \$600 million 2016 Bank of Bangladesh - \$81 million Other banks, financial institutions, casinos, cryptocurrency exchanges, SWIFT system endpoints, and ATMs in at least 38 countries worldwide



Rural Partners Network

- President Biden launched the Rural Partners Network (RPN) and assigned 13 agencies, led by the U.S Department of Agriculture, to transform the way federal agencies partner with rural places to create economic opportunity.
- There is a two pronged approach:
 1. **Depth strategy**, placing new federal staff in selected communities to provide intensive, whole-of-government, place-based technical assistance.
 2. **Breadth strategy**, deploying multiple capacity-building tools and resources that the federal government makes available to all rural places, not just selected communities.



Rural Broadband and NTIA

■ Section 5 FY21 Key Findings

- 5 agencies submitted appropriated funding to 16 programs totaling \$59.7 billion
- 10 agencies submitted obligated funding to 34 programs totaling \$8 billion
- 9 agencies submitted outlayed funding data for 37 programs totaling \$6.7 billion

■ Funding to states and tribal

- Total Funding to top state:
 - California – \$563.5 million
- Total funding to tribes - \$32.3 million
 - Digital Inclusion or Adoption - \$1.8 million
 - Infrastructure - \$27.6 million
 - Planning, Data, or Mapping - \$2.8 million



State / Local Cybersecurity Grant program

- **Infrastructure Investment and Jobs Act amended the Homeland Security Act:**
 - Appropriated **\$1B for SLTT cybersecurity grants**, FYs 2022 – 2025
 - Known as State and Local Cybersecurity Grant Program (SLCGP)
 - First-of-its-kind grant program for SLTT cybersecurity
 - Managed jointly by CISA and FEMA
 - Year 1 requires establishment of a Statewide Cybersecurity Planning Committee and the development of a Statewide Cybersecurity Plan

- **Eligibility and Funding:**
 - Eligible entities are states and territories' State Administrative Agency (SAA) with subawards to local government entities
 - Formula-based with states/territories receiving a baseline allocation plus population-based allocation
 - 80% of funds pass through to local government entities
 - 25% of total state/territory allocation must go to rural government entities
 - FY 22 SLCGP awards have been made and Cybersecurity Plans are currently under review or awaiting submission.
 - FY 23 NOFO is under development with an anticipated Summer 2023 release date.

