EMERGENCY COMMUNICATIONS COORDINATOR REPORT AUGUST 2024

Chris Maiers
August 8, 2024

CISA Entity Notifications

CISA proactively identifies information systems that contain security vulnerabilities commonly associated with ransomware attacks. After discovery, CISA notifies owners of the vulnerable systems through regional staff members (usually the CSAs) by a phone call.

Notifications contain key information regarding the vulnerable system (IP address, device name, etc.), how CISA detected it, and how it should be mitigated.

If you receive a notification, you can verify the identity of the CISA personnel through CISA Central: Central@cisa.gov or 1-844-Say-CISA (1-844-729-2472).

Having a pre-determined Out of Band email address is very helpful!!

CISA Offers No-Cost Cybersecurity Services

- **Preparedness Activities**
  - Cybersecurity Assessments
  - Cybersecurity Training and Awareness
  - Cyber Exercises and "Playbooks"
  - Cybersecurity Advisories and Alerts
  - Operational Products and Threat Indicator Sharing
  - Known Exploited Vulnerabilities (KEV) Catalog
  - Cybersecurity Performance Goals (CPGs)
  - Free Cybersecurity Tools and Services Catalog
  - Information Products and Recommended Practices

- **Response Assistance –** 24/7/365
  - Incident Coordination
  - Threat Intelligence Reporting and Information sharing
  - Malware Analysis

- **Cybersecurity State Coordinators and Cybersecurity Advisors**
  - Advisory Assistance
  - Cybersecurity Assessments
  - Incident Response Coordination
  - Working group collaboration
  - Public Private Partnership Development

Contact CISA to report a cyber incident

Call 1-888-282-0870 | email report@cisa.dhs.gov | visit https://www.cisa.gov

2024 SAFECOM Grant Guidance

- Update released June 6.
- Updated annually to provide relevant information on policies, eligible costs, technical standards, and best practices for emergency communications projects
- All entities are highly encouraged to follow the recommendations within this document to ensure interoperable, resilient, and fully effective communications.
- Grant recipients using DHS & FEMA funds for emergency comms activities must comply with SAFECOM Guidance.
- CISA.gov/safecom/funding
- https://www.cisa.gov/safecom/emergency-comms-grants-list

SAFECOM Guidance on Emergency Communications Grants

Fiscal Year 2024

U.S. Department of Homeland Security
Cybersecurity and Infrastructure Security Agency

Considerations for PS Cloud Adoption

- Highlights considerations for cloud computing adoption for public safety (PS) agencies/organizations.

- Via checklist format, the document guides practitioners through determining:
  1. Needs and scope;
  2. Requirements;
  3. Questionnaire to solicit key information.

- These considerations could assist PS organizations at any stage of cloud adoption to ensure their selection is operable, secure, resilient, and compliant with rules and regulations

- https://www.cisa.gov/news-events/news/safecom-releases-new-resource-cloud-adoption

SAFECOM®

Considerations for Public Safety Cloud Computing Adoption

Cloud-based technology solutions and their adoption by public safety organizations must meet unique mission needs. Public safety requirements may demand additional capabilities beyond the standard one-size-fits-all cloud solution. Implementing cloud-based solutions for public safety communications and data sharing requires diligent planning to ensure uninterrupted service, technology interoperability, user-tailored experience, and compliance with security, evidentiary, and resiliency requirements. For example, public safety communication needs include:

Operability: Public safety must communicate at all times and under all circumstances; organizations cannot afford any downtime

Interoperability: Public safety requires decision-making immediacy and flexibility, often paired with on-demand coordination with diverse partners; the foundation of successful partnerships is often dependent on the linking of different systems that are all governed and operated by separate entities, as authorized

Security: Public safety is increasingly seen as a prime target by malicious cyber actors seeking to compromise and disrupt communications and coordination; human errors, legacy equipment, and vulnerabilities from interconnected systems could also impact overall organizational security

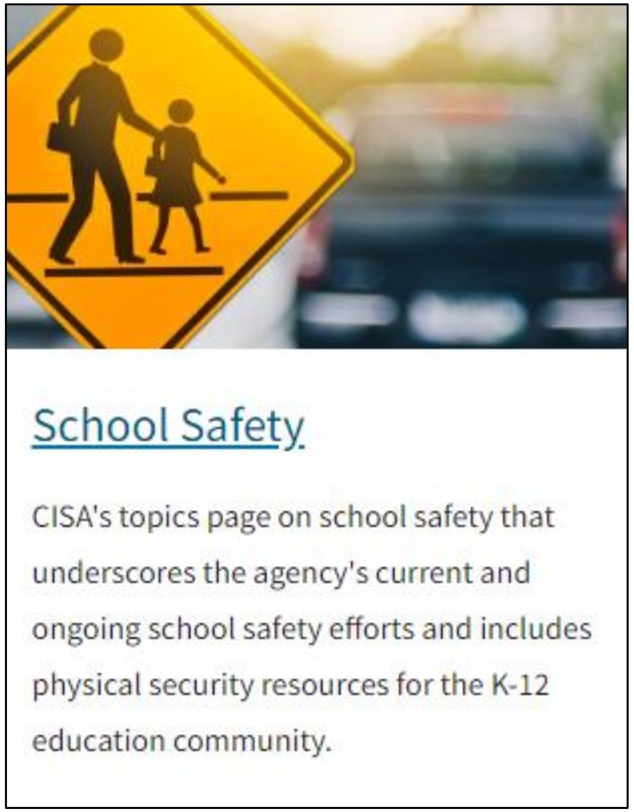
Resiliency: As mentioned above, public safety cannot afford any downtime; thus, they must maintain a separate testing environment for updates; they cannot sustain software errors or interruptions, including during patching and updates

1

cisa.gov/safecom SAFECOMgovernance@cisa.dhs.gov @CISAgov | @CISACyber @cisagov As of July 2024

School Safety Month

- Highlight resources, tools, and stakeholder events for the education community.
- Designed to enhance security measures and build resilience against various threats and hazards.
- CISA social media accounts will push out updates to tools and guidance to schools throughout August.
- Will cover cybersecurity, physical security, assessments and other assistance that may be available to schools.
- https://www.cisa.gov/topics/physical-security/school-safety/school-safety-and-cybersecurity
- https://www.schoolsafety.gov/

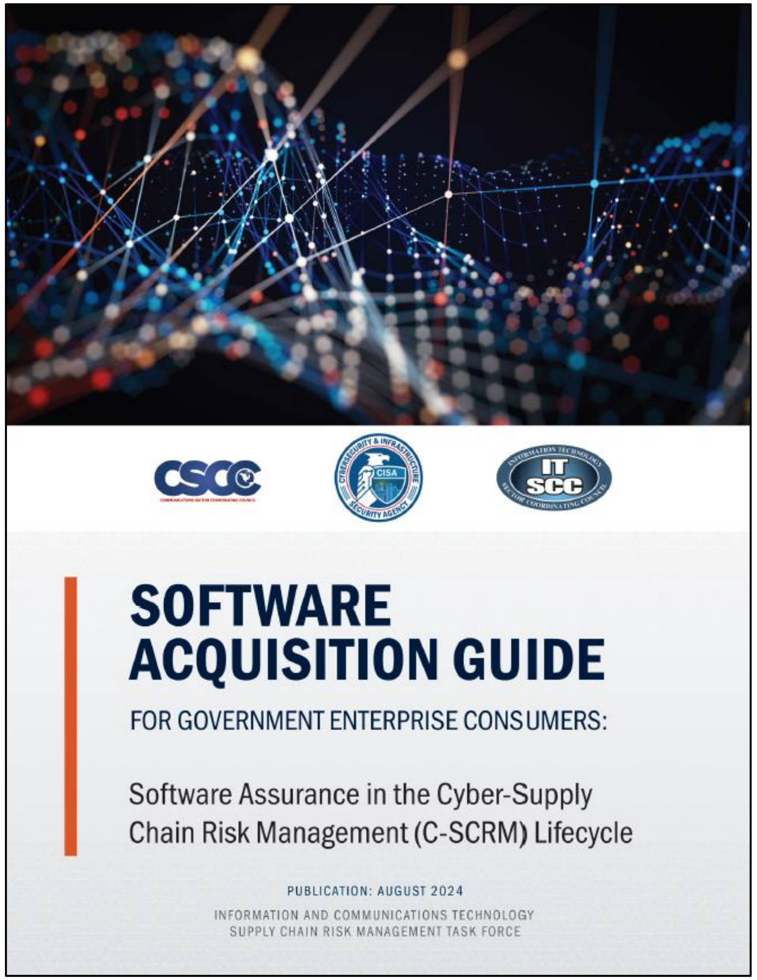


School Safety

CISA's topics page on school safety that underscores the agency's current and ongoing school safety efforts and includes physical security resources for the K-12 education community.

Software Assurance Guide for Government

- Cyberattacks have exploited vulnerabilities and weaknesses in software and within software supply chains.
- This guide consolidates relevant software assurance guidance & frameworks into a single document.
- Enables easy navigation through requirements in a clear, concise manner.
- Encompasses all types of software, including commercial, open source, contracted, and cloud-based solutions, used within and by the government.
- https://www.cisa.gov/resources-tools/resources/software-acquisition-guide-government-enterprise-consumers-software-assurance-cyber-supply-chain



SOFTWARE ACQUISITION GUIDE

FOR GOVERNMENT ENTERPRISE CONSUMERS:

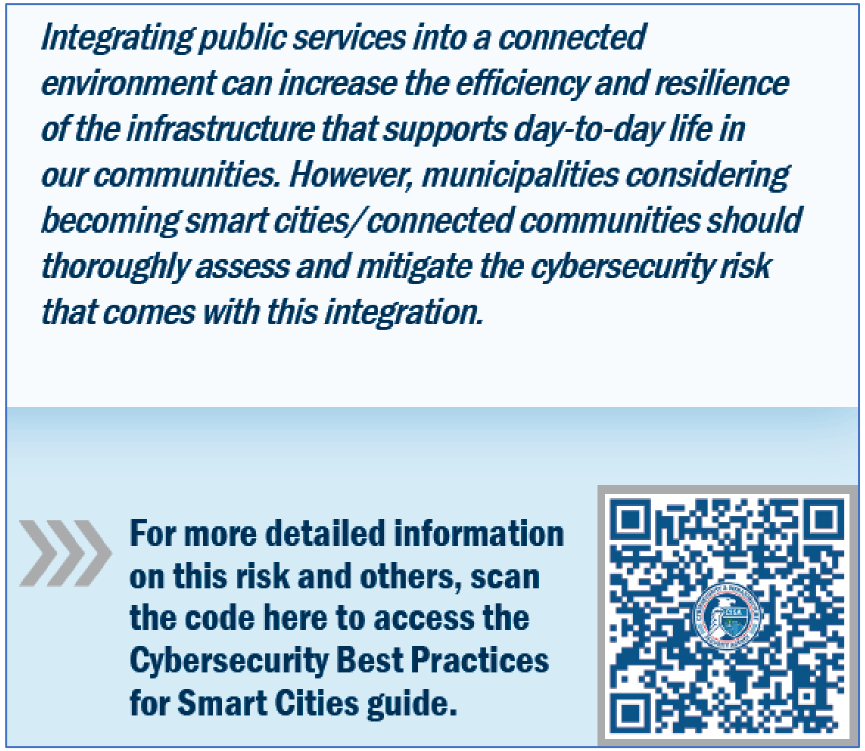
Software Assurance in the Cyber-Supply Chain Risk Management (C-SCRM) Lifecycle

PUBLICATION: AUGUST 2024

INFORMATION AND COMMUNICATIONS TECHNOLOGY
SUPPLY CHAIN RISK MANAGEMENT TASK FORCE

Connected Communities Risk Postcard Series

- Released on August 2, 2024.
- Each postcards features one of the three risks to connected communities/smart cities outlined in the Cybersecurity Best Practices for Smart Cities Guide.
- Also includes appropriate mitigation recommendations for each risk. The risk postcard series includes:
  - *Connected Communities Risk: Expanded and Interconnected Attack Surface*
  - *Connected Communities Risk: ICT Supply Chain and Vendors*
  - *Connected Communities Risk: Automation of Operations*
- https://www.cisa.gov/resources-tools/resources/connected-communities-risk-postcards

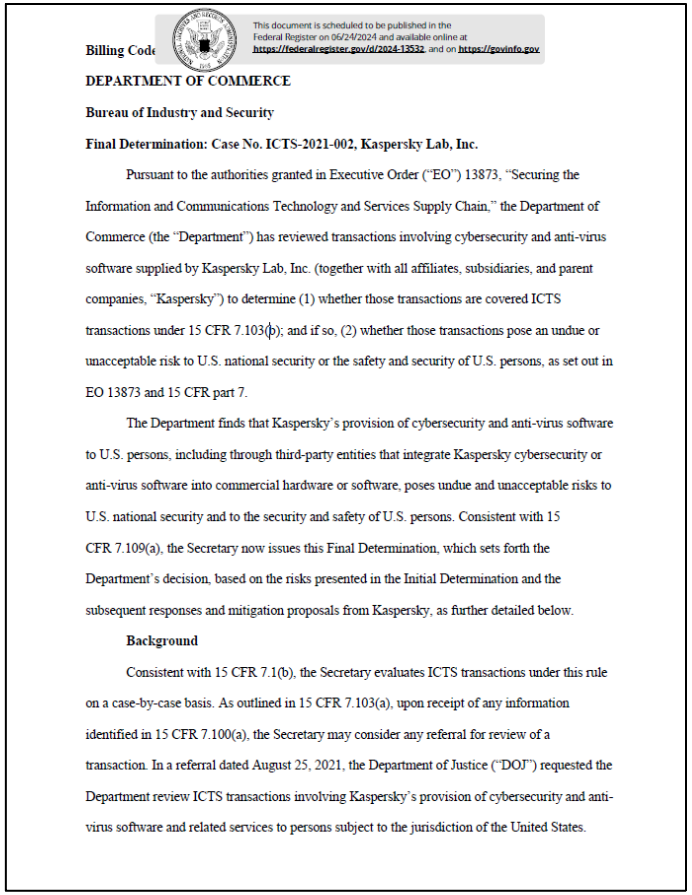


Integrating public services into a connected environment can increase the efficiency and resilience of the infrastructure that supports day-to-day life in our communities. However, municipalities considering becoming smart cities/connected communities should thoroughly assess and mitigate the cybersecurity risk that comes with this integration.

For more detailed information on this risk and others, scan the code here to access the Cybersecurity Best Practices for Smart Cities guide.

Updates on Foreign Software/Hardware

- Department of Commerce has ruled against Kaspersky products via Final Determination (Case No. ICTS-2021-002).
  - Added to prohibited list due to security concerns and applies to government and private customers in the United States.
  - List in appendices includes current products but is not exhaustive.
  - Published in *Federal Register*: https://federalregister.gov/d/2024-13532
- Complete list of device and software suppliers outlined List of Equipment and Services Covered By Section 2 of The Secure Networks Act: https://www.fcc.gov/supplychain/coveredlist



This document is scheduled to be published in the Federal Register on 06/24/2024 and available online at https://federalregister.gov/d/2024-13532, and on https://govinfo.gov

Billing Code

DEPARTMENT OF COMMERCE

Bureau of Industry and Security

Final Determination: Case No. ICTS-2021-002, Kaspersky Lab, Inc.

Pursuant to the authorities granted in Executive Order ("EO") 13873, "Securing the Information and Communications Technology and Services Supply Chain," the Department of Commerce (the "Department") has reviewed transactions involving cybersecurity and anti-virus software supplied by Kaspersky Lab, Inc. (together with all affiliates, subsidiaries, and parent companies, "Kaspersky") to determine (1) whether those transactions are covered ICTS transactions under 15 CFR 7.103(b); and if so, (2) whether those transactions pose an undue or unacceptable risk to U.S. national security or the safety and security of U.S. persons, as set out in EO 13873 and 15 CFR part 7.

The Department finds that Kaspersky's provision of cybersecurity and anti-virus software to U.S. persons, including through third-party entities that integrate Kaspersky cybersecurity or anti-virus software into commercial hardware or software, poses undue and unacceptable risks to U.S. national security and to the security and safety of U.S. persons. Consistent with 15 CFR 7.109(a), the Secretary now issues this Final Determination, which sets forth the Department's decision, based on the risks presented in the Initial Determination and the subsequent responses and mitigation proposals from Kaspersky, as further detailed below.

Background

Consistent with 15 CFR 7.1(b), the Secretary evaluates ICTS transactions under this rule on a case-by-case basis. As outlined in 15 CFR 7.103(a), upon receipt of any information identified in 15 CFR 7.100(a), the Secretary may consider any referral for review of a transaction. In a referral dated August 25, 2021, the Department of Justice ("DOJ") requested the Department review ICTS transactions involving Kaspersky's provision of cybersecurity and anti-virus software and related services to persons subject to the jurisdiction of the United States.

Regional News of Note

- Communications Exercises:
  - Central States COMMEX – Joplin (MO)/Quapaw (OK) from September 10-13, 2024
- Interoperability Markers update meeting requests sent out.
  - Scheduled August 9, 2024, at 1100 CT.

For more information:

Chris Maiers
Christopher.Maiers@cisa.dhs.gov
202-701-3235

Jim Hoflen
james.hoflen@cisa.dhs.gov
515-707-0332