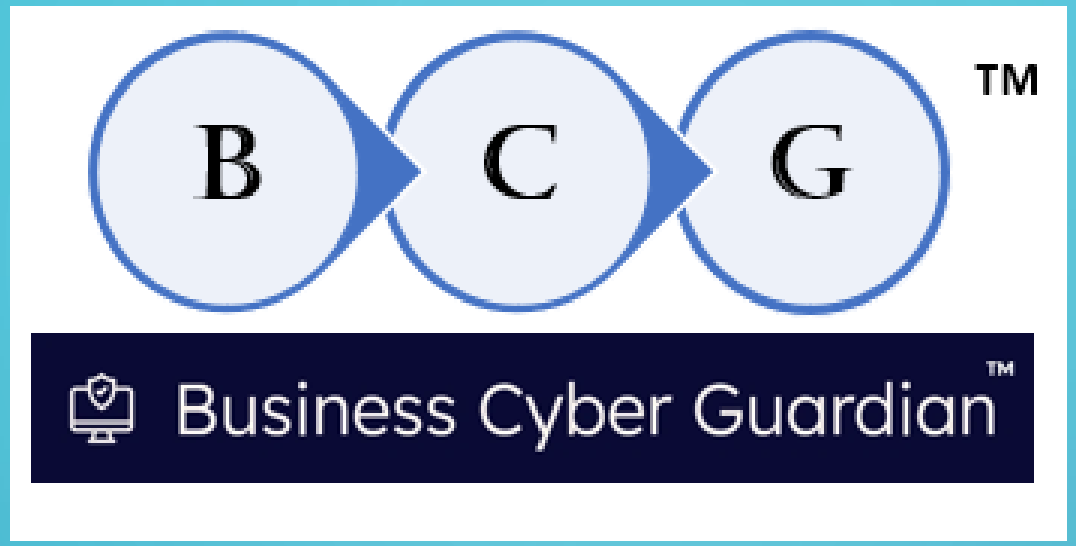


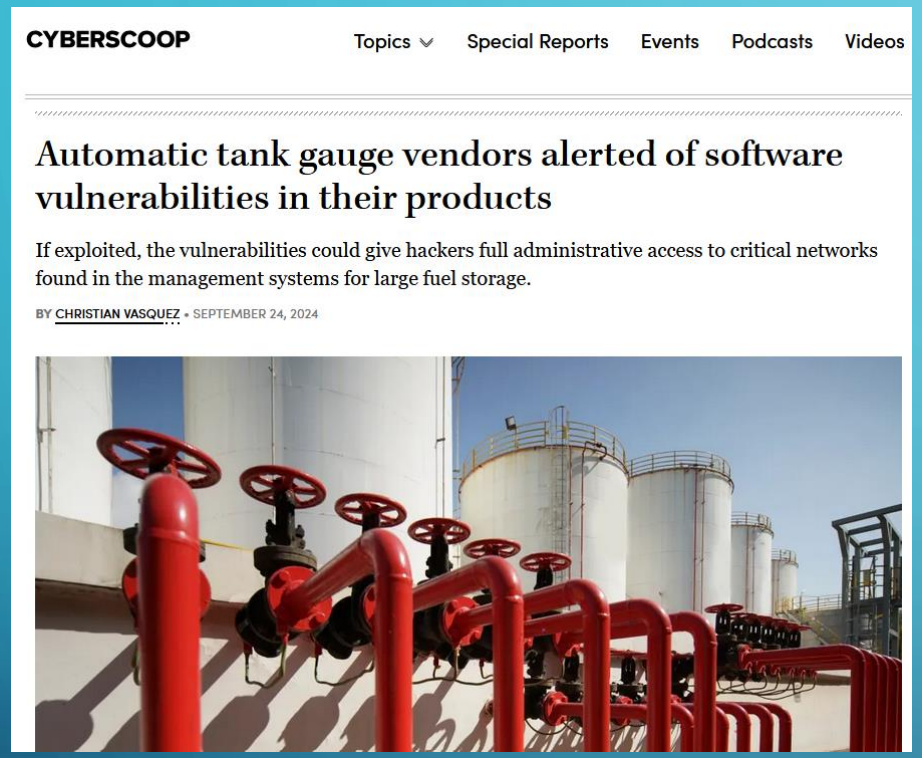
CISA SECURE BY DESIGN GOALS AND OBJECTIVES

Dick Brooks, Lead Software Engineer SAG-PM and SAG-CTR
dick@businesscyberguardian.com

INTRODUCTION

- Dick is one of the co-authors of CISA's Secure Software Acquisition Guide and a leading technical advisor on Software Supply Chain Risk Management practices across Critical Infrastructure
- He serves on two Critical Infrastructure Sector Risk Management Agencies (SRMA) Critical Manufacturing Sector and the Healthcare Sector
- He is a Co-Founder and lead software engineer for Business Cyber Guardian and the Software Assurance Guardian product line (SAG-PM and SAG-CTR)

YOU DON'T HAVE TO LOOK FAR FOR RISKS IN SOFTWARE



Many well-known attacks have exploited vulnerabilities and weaknesses in software and within software supply chains; an issue that spans both proprietary and open-source software which impacts both private sector and government enterprises.

WHAT IT MEANS TO BE SECURE BY DESIGN

- Products designed with Secure by Design principles **prioritize the security of customers as a core business requirement**, rather than merely treating it as a technical feature
- Companies should implement Secure by Design principles to **significantly decrease the number of exploitable flaws before introducing them to the market** for widespread use or consumption.
- **Out-of-the-box, products should be secure** with additional security features such as multi-factor authentication (MFA), logging, and single sign-on (SSO) available at no extra cost.

GOALS – THE WHAT

- Transparency of software manufacturing processes
- Accountability for customer safety
- Organization Commitment and Support

SOFTWARE PRODUCT SECURITY PRINCIPLES

Software manufacturers are encouraged to adopt a strategic focus that prioritizes software security. The authoring organizations developed the following three core principles to guide software manufacturers in building software security into their design processes prior to development, configuration, and shipment of their products.

1 **Take ownership of customer security outcomes** and evolve products accordingly. The burden of security should not fall solely on the customer.

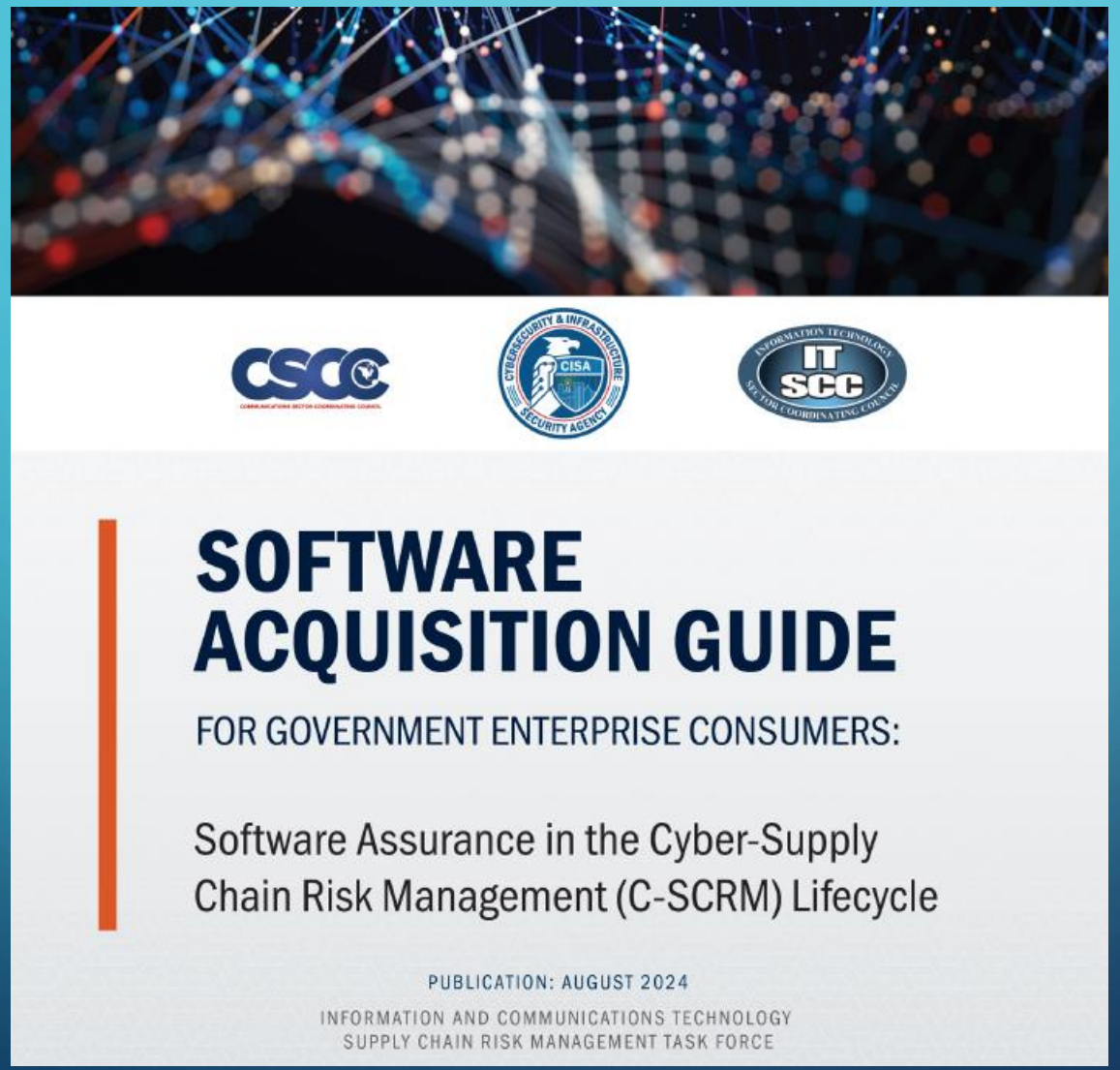
2 **Embrace radical transparency and accountability.** Software manufacturers should pride themselves in delivering safe and secure products, as well as differentiating themselves from the rest of the manufacturer community based on their ability to do so. This may include sharing information they learn from their customer deployments, such as the uptake of strong authentication mechanisms by default. It also includes a strong commitment to ensure vulnerability advisories and associated common vulnerability and exposure (CVE) records are complete and accurate. However, beware of the temptation to count CVEs as a negative metric, since such numbers are also a sign of a healthy code analysis and testing community.

3 **Build organizational structure and leadership to achieve these goals.** While technical subject matter expertise is critical to product security, senior executives are the primary decision makers for implementing change in an organization. Executives need to prioritize security as a critical element of product development across the organization, and in partnership with customers.

SIMILAR TO RESTAURANT TRUST SCORING PRINCIPLES

- Provide consumers with visibility into trustworthiness before buying
- Incentivize good practices to produce secure products
- Risk always exists, but trust must be earned
- Risk ALWAYS exists, but trust DOESN'T ALWAYS exist
- Correlates well with other industry practices for transparency and trust
  - New York City Restaurant Trust Scores indicating adherence to good practices provides consumers with advance warning of risky restaurants versus trustworthy establishments
  - "Almost everywhere she worked, there were outbreaks of typhoid."

THE HOW – SECURE SOFTWARE ACQUISITION

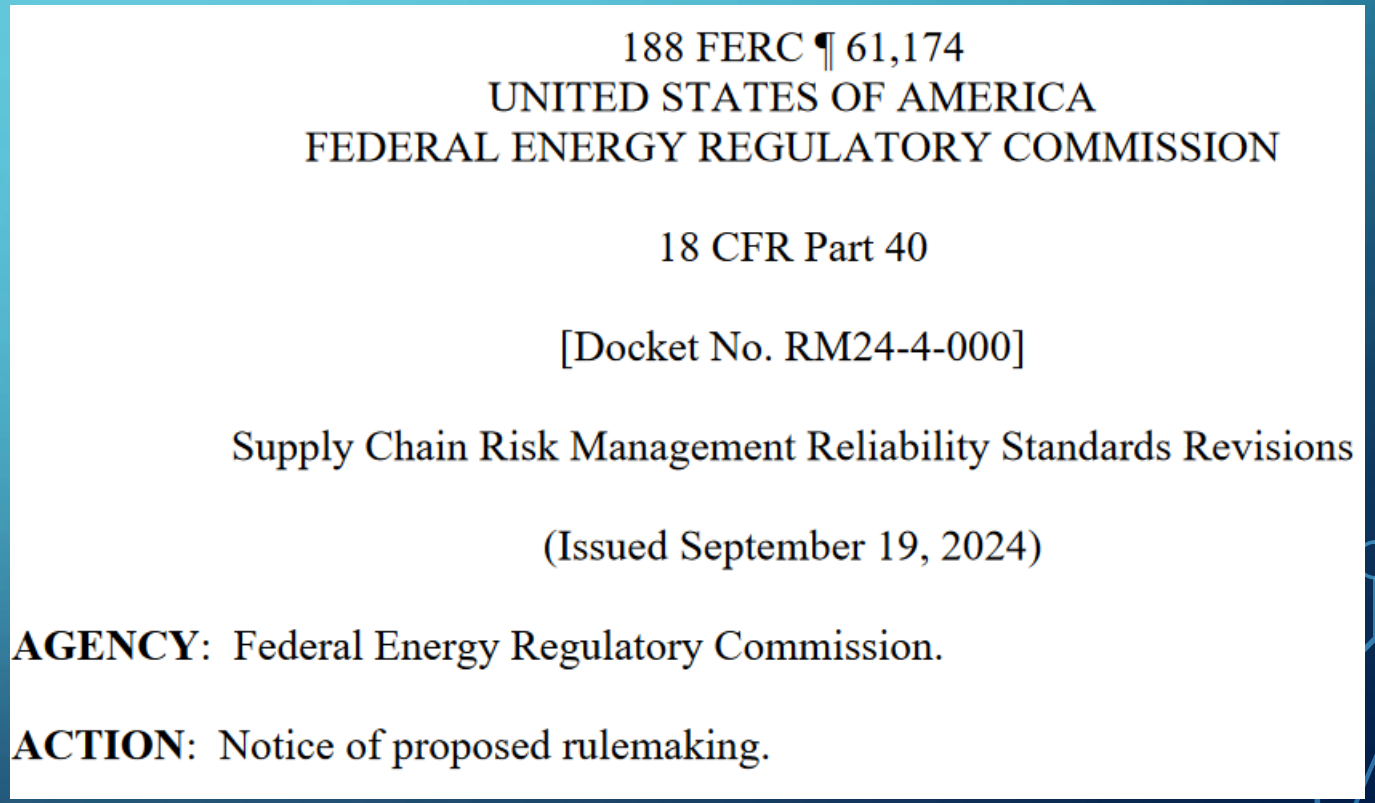


CONSUMERS CAN DETERMINE TRUSTWORTHINESS

- Risk always exists, but trust must be earned and awarded
- How to verify software vendors and products are "Secure by Design"
  1. Download CISA's Software Assurance Guide Spreadsheet
  2. Send the spreadsheet to vendors asking to answer the 19 Governance questions
  3. Evaluate the responses to determine which vendors are following Secure by Design practices (specified in the Guide and Spreadsheet)
  4. Determine which vendors and products are trustworthy, and which are not; award trust wisely – you own the risks and impacts that come with cyber attacks
  5. Never trust software, always verify and report!™
  6. Look both ways before buying and installing software products

REGULATIONS ARE HERE AND MORE ARE COMING

- SEC: 17 CFR 229.106
- FERC: Docket RM24-4-000



188 FERC ¶ 61,174
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

18 CFR Part 40

[Docket No. RM24-4-000]

Supply Chain Risk Management Reliability Standards Revisions

(Issued September 19, 2024)

AGENCY: Federal Energy Regulatory Commission.

ACTION: Notice of proposed rulemaking.

RESOURCES

- https://www.cisa.gov/resources-tools/resources/software-acquisition-guide-government-enterprise-consumers-software-assurance-cyber-supply-chain
- https://www.cisa.gov/securebydesign
- https://www.ecfr.gov/current/title-17/chapter-II/part-229/subpart-229.100/section-229.106
- https://www.ferc.gov/media/e-1-rm24-4-000
- https://home.nyc.gov/site/doh/business/food-operators/letter-grading-for-restaurants.page
- Business Cyber Guardian website: https://businesscyberguardian.com/