We provide a secure, reliable, and affordable delivery platform that binds together every commercial and residential address in the nation.

484 million mailpieces daily

232,000 vehicles

31,000 retail Post Offices

There’s more to the Postal Service than our physical footprint. We’re looking to connect the nation in the digital age through a range of innovative offerings.
We maintain one of the **largest information technology networks in the world**. Our technology resources enable us to deliver value in the digital age, but also expose our enterprise to cybersecurity risk.
Cyberattacks have increased in frequency, sophistication, and impact. These attacks pose a significant risk to organizations, often leading to operational disruptions and loss of corporate and/or personal data.

**Average enterprise cost of a ransomware attack**: $5 million

**Average time it takes organization to identify a data breach**: 191 days

**Percentage of companies that experienced an industrial control security incident in 2018**: 54%

**Percentage of companies that experienced an Internet of Things (IoT) security incident in 2018**: 61%
CISO develops, implements, and manages rigorous cybersecurity processes and technologies to protect USPS networks, monitor cybersecurity threats, and respond to cybersecurity incidents.

**VISION**

Become a leader in cybersecurity to **protect the information of the United States Postal Service** – the network that binds the nation.

**MISSION**

To **support and protect** the U.S. Postal Service and its employees, information, technology assets, and customers by:

1. **Detecting, preventing, responding to,** and **investigating** incidents of cybercrime and misuse of information technology assets
2. **Directing**, in conjunction with the **U.S. Postal Inspection Service (USPIS)**, the investigative response to violations of laws that defend the nation's mail system from cybercrime and misuse
3. **Coordinating** the enforcement of laws to defend the USPS mail system
The CyberSafe Guardian program leverages a network of volunteers to create a “cybersafe” culture across the Postal Service.

### Purpose

- **Guardians serve as local facility representatives across the Postal Service**
- **Provide cybersecurity information** and guidance directly to the field
- **Promote cybersafe behavior** by demonstrating best practices
- **Serve as partners** on the ground and provide CyberSafe with field perspective and feedback

### Overview and Scope

The program includes the following components:

- **Nation-wide network of 108 EAS employees**, including IT specialists and managers
- **Monthly calls** to provide information on high-priority cyber topics and gather feedback
- **Shareable materials and tools** to help Guardians spread the word

CyberSafe Guardians lend a human element to the CyberSafe at USPS® program and help drive cybersafe behavior change.
Starting with just seven initial states, the CyberSafe Guardians program has expanded to 108 representatives across 38 states and two territories.

108 Guardians consisting of EAS employees, including IT specialists and managers.

38 states represented around the country, plus Guam and Puerto Rico.

12 calls per year to provide information on high-priority cyber topics and gather feedback.

4 hours of average time Guardians spend per month on awareness activities.

Key Guardian Activities:

- **Provide cybersecurity information** and guidance directly to the field.
- **Promote cybersafe behavior** by demonstrating best practices.
- **Serve as partners** in your facilities, providing CyberSafe at USPS® with field perspective and feedback.

Denotes state with active Guardian.
If you have questions about the CyberSafe Guardians program, please reach out to us!

CyberSafe at USPS®
CyberSafeComms@usps.gov

Questions?