SUPPLY MANAGEMENT

USPS | Re:Supply

NEWSLETTER

ISSUE 35| December 2021

Mark Guilfoil
Vice President, Supply Management

Cybersecurity Announcement- Log4j Vulnerability Impact Assessment

To: All U.S. Postal Service Suppliers

You are receiving this newsletter from the Postal Service as you have registered your interest to do business with the Postal Service or your email address is on file as a point of contact for a current or past contract. Please share this newsletter with your colleagues within your company as it contains important supplier related information about the Postal Service.

The Cybersecurity and Infrastructure Security Agency (CISA) recently announced a widespread security vulnerability (CVE-2021-44228) impacting the Apache's Log4j software library, known as "Log4Shell" and "Logjam." Log4j is broadly used in a variety of consumer and enterprise services, websites, and applications —as well as in operational technology products—to log security and performance information.

The U.S. Postal Service (Postal Service) Corporate Information Security Office (CISO) wants to ensure that our suppliers are aware of and are tracking this vulnerability in their own environments. We encourage each organization to follow the guidance provided by CISA to remediate this vulnerability, protecting your organization as well as your customers and business partners. Your action is needed as discussed below, and which will directly support our efforts to securely and timely deliver Peak Season for all our customers.

The Postal Service depends on many third-party suppliers to perform and support critical functions and operational systems. In doing so, we have a reliance on many organizations. Accordingly, it is imperative for the Postal Service to understand any potential impacts to our data, systems, services, and assets that may arise due to the Log4j vulnerability. Therefore, we ask that you complete an IMPACT ASSESSMENT using the following link:

LIVE CISO Survey

As a supplier, in accordance with your contractual obligations, we would also like to remind you that you are required to timely report any security incidents that could impact Postal Service data, systems, or services to the contracting officer and CyberSafe at cybersafe@usps.gov.

We value the relationship between our organizations and appreciate your assistance in this matter.

Mark A. Guilfoil
Vice President, Supply Management

SUPPLY MANAGEMENT

USPS | Re:Supply

NEWSLETTER

ISSUE 35 | December 2021

ARE YOU REGISTERED TO DO BUSINESS WITH THE U.S. POSTAL SERVICE?

All suppliers interested in doing business with the U.S. Postal Service should register their company in the Postal Service Supplier Registration system.

For more information, please go to http://about.usps.com/suppliers/becoming/registration.htm

Save and Grow with the USPS® Loyalty Program

The U.S Postal Service has introduced USPS® Loyalty, a new program designed to reward small businesses and frequent users of Click-N-Ship with incentives for dollars spent on Priority Mail® and Priority Mail Express. To learn more about the USPS Loyalty Program go to https://www.usps.com/business/loyalty.htm?utm

Or contact USPSLoyaltyProgram@usps.com for questions or assistance.

CONTACT US!

We value your questions and feedback to this newsletter. Please feel free to reply to this message with your feedback or mail to:

U.S. Postal Service
Supply Management Communications
475 L'Enfant Plaza, SW, Room 1100
Washington, DC 20260-6201

If you prefer not to receive future issues of *re:supply* from the U.S. Postal Service, click SMCommunications@usps.gov