# MITIGATE CYBERSECURITY RISKS WITH PRE-TESTED SOFTWARE UPDATES

## PROTECT MISSION-CRITICAL COMMUNICATION SYSTEMS

### COMMUNICATION SYSTEMS FACE INCREASED CYBERSECURITY RISKS

As dependency on IP-based systems increases, the risk of intrusion and system compromise becomes an even greater challenge. As mission-critical communications systems become interconnected to other IP-based systems, they are further exposed to continuously evolving cybersecurity threats.

### MAINTAIN COMPLIANCE

Pre-testing and validation procedures enable adherence to various government mandates, specific market regulations and industry best practices set for increased system cybersecurity measures including:

- Federal Information Security Management Act (FISMA)
- Department of Defense Information Assurance Certification and Accreditation Process (DIACAP)
- Department of Homeland Security Policy 4300A
- National Institute of Standards Technology: NIST 800-53
- North American Electric Reliability Corporation (NERC)
- ISO 27001
- Payment Card Industry (PCI) Security Standards
- Other privacy directives

### PRE-TEST SOFTWARE UPDATES TO PROTECT CONTINUITY OF SYSTEM OPERATIONS

Robust system patching capability is an integral part of the overall organization's cybersecurity program. Industry best practices suggest that software patches are applied as soon as possible after release from the vendor. However, testing software updates before deploying on a mission critical system is absolutely essential.

Motorola's Security Update Service (SUS) pre-tests the latest anti-malware definitions and all applicable software patches in dedicated test labs. Only the applicable patches needed for the system are identified and selected for testing. This validates that no unnecessary software is introduced via the patching process. Once validated as safe for deployment with the radio network, the updates can be deployed for you by Motorola; or made available to you on Motorola's secure extranet site for implementation.

Rely on Motorola's certified security experts to identify and validate the necessary updates required to maintain cybersecurity readiness. Security Update Service ensures the right patches are identified, validated and applied in a timely manner to minimize cybersecurity risk and increase the operational integrity of your mission critical communications system.

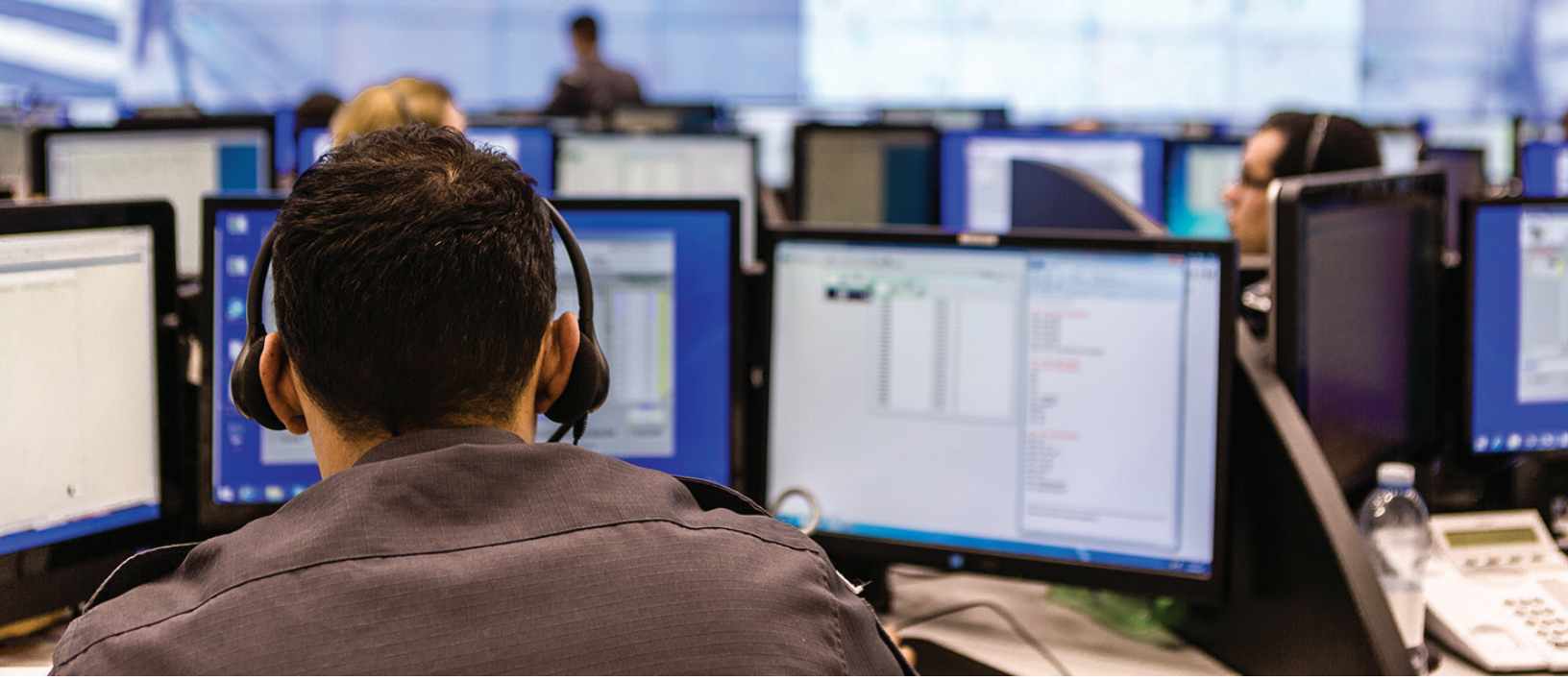
**CYBER ATTACKS**

**600%** GROWTH IN LATIN AMERICA IN 2021

**SECURITY BREACHES**

**110%** THE AVERAGE COST INCREASED IN 2021

REMOTE WORK DUE TO COVID-19 WAS ONE OF THE MOST IMPACTING CAUSES



## MINIMIZE RISK – AND COSTS

Security Update Service delivers:

**Increased network availability**
Reduce the vulnerabilities addressed by security patches and increase the safeguards of confidentiality, integrity, and availability of mission-critical systems.

**Reduced maintenance costs**
Dramatically reduce potential for system downtime; resulting in fewer maintenance costs to restore the system back to proper operational state.

**Assurance**
Motorola assumes responsibility to verify security updates without unnecessary burden to your staff.

**Better use of technical resources**
Keep staff focused on core responsibilities relying on Motorola to deliver the expertise and support for a proper cybersecurity regimen.

## DELIVERY OPTIONS

Two options are available for deploying security updates onto your radio network once software is pre-tested.

**Customer download**
Latest security updates are made available via Motorola's secure extranet site for your team to download and install onto your radio network.

**Remote SUS delivery**
Motorola's dedicated staff remotely installs the security updates onto your radio network. Vulnerabilities from third party software are addressed as soon as the validation of recommended patches is completed. We will also provide reports outlining updates made for your team's review and awareness.

**Coming soon**
**ON-SITE PATCH DELIVERY SERVICE**
Let us take care of your entire patch and reboot requirements on-site. We will address vulnerabilities from third-party software, and if a patch fails, develop a plan and then redeploy. Our robust patch deployment reporting tool keeps your team, management, auditors and regulators fully informed.

For more information about Security Services, contact your Motorola Solutions representative or visit motorolasolutions.com/services

MOTOROLA SOLUTIONS

Motorola Solutions, Inc. 500 West Monroe Street, Chicago, Il 60661 U.S.A. **motorolasolutions.com**