POMS RISK CONTROL & INSURANCE
SMARTER INSURANCE FOR SMARTER BUSINESS.

New Mexico Public Schools Insurance Authority

In light of the recent events in Ukraine and Russia, as well as the current cybersecurity environment, the US Government has released more information on cybersecurity.

Below are some informative articles:

- Russia Cyber Threat Overview and Advisories
- SHIELDS UP Guidance for All Organizations

In addition, the Cybersecurity and Infrastructure Security Agency (CISA) has compiled a list of **free cybersecurity tools and services** to help organizations further advance their security capabilities.

These resources are categorized according to the four goals outlined in CISA Insights: Implement Cybersecurity Measures Now to Protect Against Critical Threats:

1. Reducing the likelihood of a damaging cyber incident;
2. Detecting malicious activity quickly;
3. Responding effectively to confirmed incidents; and
4. Maximizing resilience.

Foundational Measures

All organizations should take certain foundational measures to implement a strong cybersecurity program:

- **Fix the known security flaws in software.** Check the CISA Known Exploited Vulnerabilities (KEV) Catalog for software used by your organization and, if listed, update the software to the latest version according to the vendor's instructions. **Note:** CISA continually updates the KEV catalog with known exploited vulnerabilities.

- **Implement multifactor authentication (MFA).** Use multifactor authentication where possible. MFA is a layered approach to securing your online accounts and the data they contain. When you enable MFA in your online services (like email), you must provide a combination of two or more authenticators to verify your identity before the service

grants you access. Using MFA protects your account more than just using a username and password. Why? Because even if one factor (like your password) becomes compromised, unauthorized users will be unable to meet the second authentication requirement, ultimately stopping them from gaining access to your accounts.

- **Halt** bad practices**.** Take immediate steps to: (1) replace end-of-life software products that no longer receive software updates; (2) replace any system or products that rely on known/default/unchangeable passwords; and (3) adopt MFA (see above) for remote or administrative access to important systems, resources, or databases.

- **Sign up for CISA's Cyber Hygiene Vulnerability Scanning.** Register for this service by emailing vulnerability@cisa.dhs.gov. Once initiated, this service is mostly automated and requires little direct interaction. CISA performs the vulnerability scans and delivers a weekly report. After CISA receives the required paperwork, scanning will start within 72 hours and organizations will begin receiving reports within two weeks. **Note:** vulnerability scanning helps secure internet-facing systems from weak configurations and known vulnerabilities and encourages the adoption of best practices.

- **Get your Stuff Off Search (S.O.S.).** While zero-day attacks draw the most attention, frequently, less complex exposures to both cyber and physical security are missed. Get your Stuff Off Search–S.O.S.–and reduce internet attack surfaces that are visible to anyone on web-based search platforms.

If you have any questions, please feel free to contact us:

Jo Anne Roque, Vice President - Account Management
Direct: (818) 449-9369
Toll Free: (800) 578-8802, ext. 369

Lynn Solomon, Vice President-Account Executive
Direct: (818) 449-9372
Toll Free: (800) 578-8802, ext. 372

Justin Perkins, Director
Direct: (818) 449-9301
Toll Free: (800) 578-8802, ext. 301

POMS RISK CONTROL & INSURANCE
SMARTER INSURANCE FOR SMARTER BUSINESS.