CIS™ Center for Internet Security®

MS-ISAC Multi-State Information Sharing & Analysis Center

Federally-funded Cyber Threat Resources for State, Local and Tribal Governments

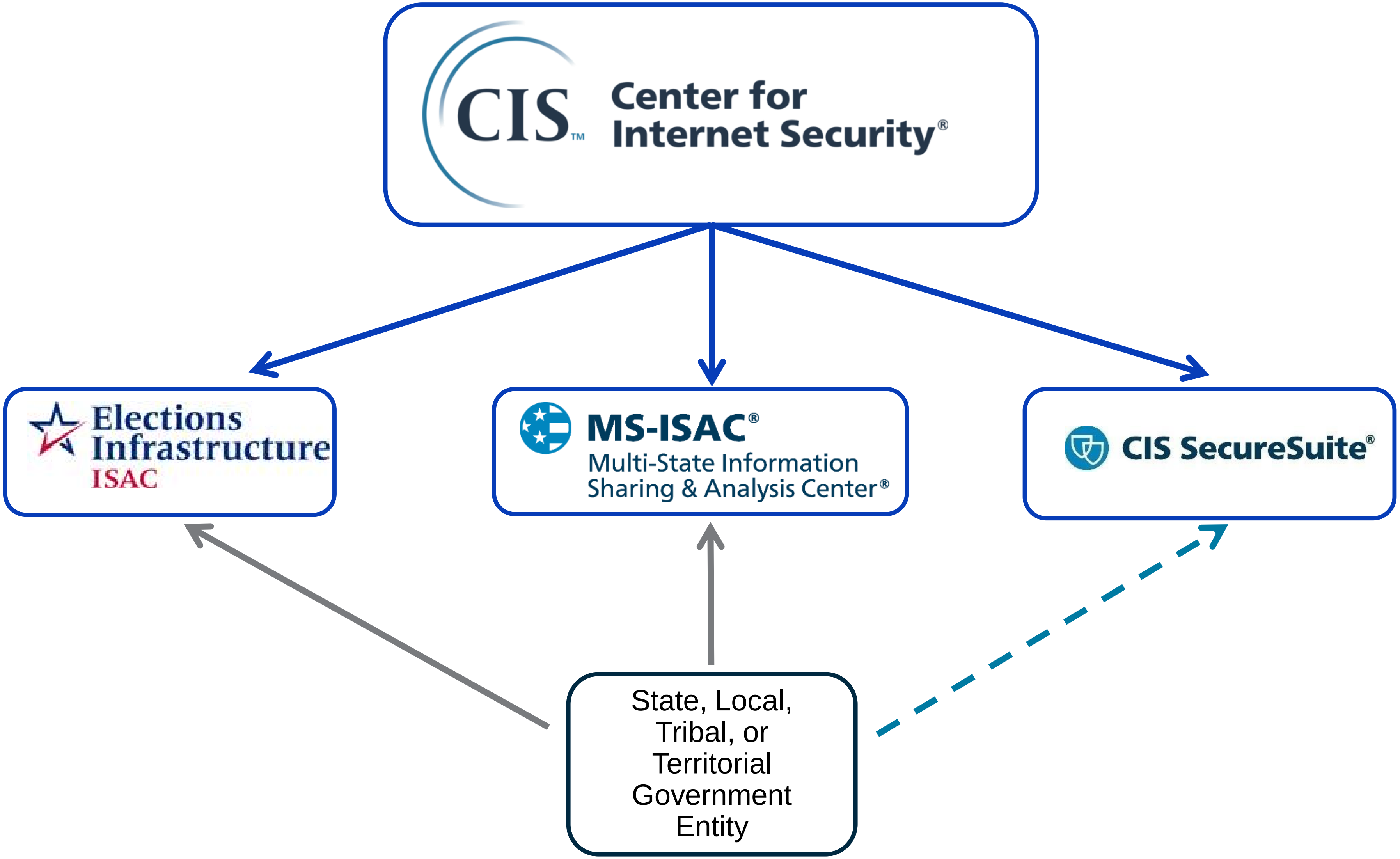
Greta Noble

Senior Program Specialist

MS-ISAC

518.880.0740

Greta.noble@cisecurity.org



CIS Center for Internet Security®

Elections Infrastructure ISAC

MS-ISAC® Multi-State Information Sharing & Analysis Center®

CIS SecureSuite®

State, Local, Tribal, or Territorial Government Entity

TLP: WHITE

Who We Serve

State, Local, Tribal, and Territorial Governments

- 50 State Governments
- 5,700+ Local Governments
- 6 Territorial Governments
- 93 Tribal Governments
- 79 DHS-recognized Fusion Centers

Local Governments

- K-12 School Districts, Higher Education
- Law Enforcement, Cities, Public Authorities
- Libraries, Public Health, Airports
- 41 Alaskan Members

How to access MS-ISAC resources

- Register for the MS-ISAC's services here:

https://learn.cisecurity.org/ms-isac-registration

- The MS-ISAC Stakeholder Engagement team will provide you with next steps

24 x 7 Security Operations Center

Central location to report any cybersecurity incident

- **Support:**
  - Network Monitoring Services
  - Research and Analysis
- **Analysis and Monitoring:**
  - Threats
  - Vulnerabilities
  - Attacks
- **Reporting:**
  - Cyber Alerts & Advisories
  - Web Defacements
  - Account Compromises
  - Hacktivist Notifications

To report an incident or request assistance:

Phone: 1-866-787-4722

Email: soc@cisecurity.org

TLP: WHITE

Computer Emergency Response Team

- Incident Response (includes on-site assistance)
- Network & Web Application Vulnerability Assessments
- Malware Analysis
- Computer & Network Forensics
- Log Analysis
- Statistical Data Analysis

To report an incident or request assistance:
Phone: 1-866-787-4722
Email: soc@cisecurity.org

TLP: WHITE

Monitoring of IP Range & Domain Space

IP Monitoring

- IPs connecting to malicious C&Cs
- Compromised IPs
- Indicators of compromise from the MS-ISAC network monitoring (Albert)
- Notifications from Spamhaus

Domain Monitoring

- Notifications on compromised user credentials, open source and third party information
- Vulnerability Management Program (VMP)

Send domains, IP ranges, and contact info to:
soc@cisecurity.org

TLP: WHITE

Vulnerability Management Program

Web Profiler

- ✓Server type and version (IIS, Apache, etc.)
- ✓Web programming language and version (PHP, ASP, etc.)
- ✓Content Management System and version (WordPress, Joomla, Drupal, etc.)

Email notifications are sent with 2 attachments containing information on out-of-date and up-to-date systems:

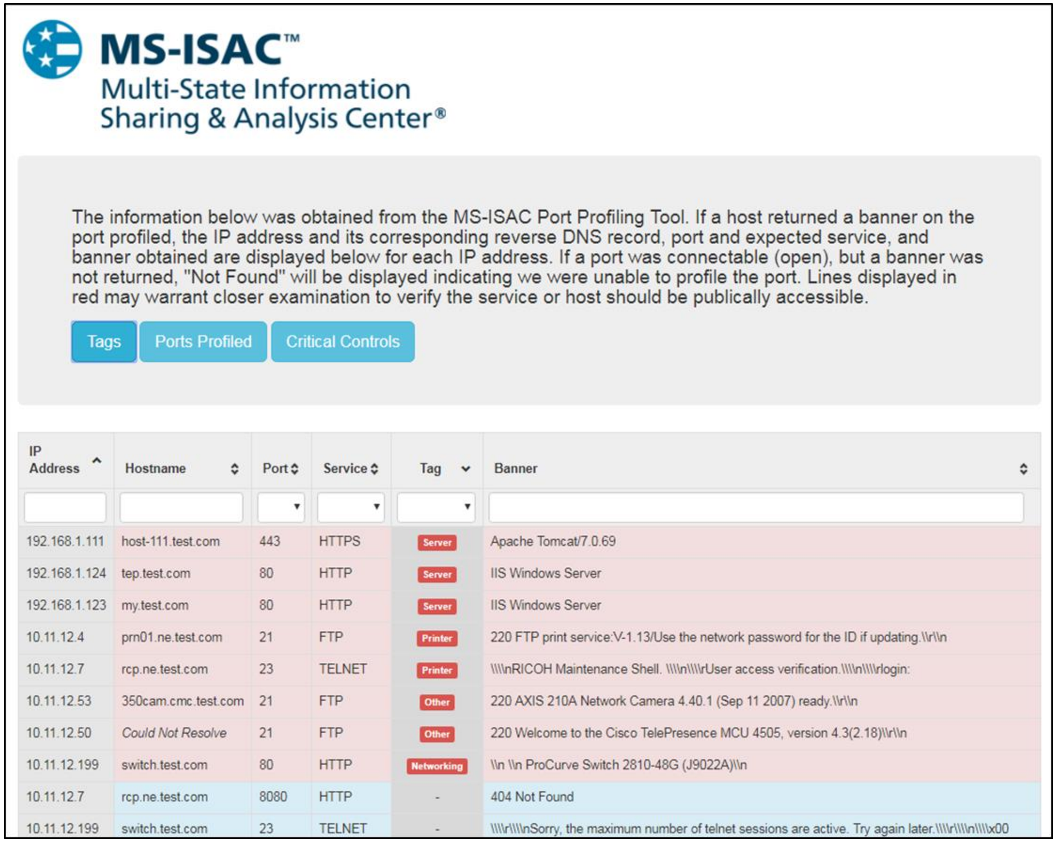
- Out-of-Date systems should be patched/updated and could potentially have a vulnerability associated with it
- Up-to-Date systems have the most current patches

TLP: WHITE

Vulnerability Management Program

Port Profiler

- **MS-ISAC will connect to 12 common ports on public IPs provided for our monitoring program.**
- **Quarterly notifications**
- **Contact vmp.dl@cisecurity.org**
- **Source IP address: 52.14.79.150**



MS-ISAC™
Multi-State Information Sharing & Analysis Center®

The information below was obtained from the MS-ISAC Port Profiling Tool. If a host returned a banner on the port profiled, the IP address and its corresponding reverse DNS record, port and expected service, and banner obtained are displayed below for each IP address. If a port was connectable (open), but a banner was not returned, "Not Found" will be displayed indicating we were unable to profile the port. Lines displayed in red may warrant closer examination to verify the service or host should be publically accessible.

IP Address	Hostname	Port	Service	Tag	Banner
192.168.1.111	host-111.test.com	443	HTTPS	Server	Apache Tomcat/7.0.69
192.168.1.124	tep.test.com	80	HTTP	Server	IIS Windows Server
192.168.1.123	my.test.com	80	HTTP	Server	IIS Windows Server
10.11.12.4	prn01.ne.test.com	21	FTP	Printer	220 FTP print service:V-1.13/Use the network password for the ID if updating.\\r\\n
10.11.12.7	rcp.ne.test.com	23	TELNET	Printer	\\\\nRICOH Maintenance Shell. \\\\n\\\\rUser access verification.\\\\n\\\\rlogin:
10.11.12.53	350cam.cmc.test.com	21	FTP	Other	220 AXIS 210A Network Camera 4.40.1 (Sep 11 2007) ready.\\r\\n
10.11.12.50	*Could Not Resolve*	21	FTP	Other	220 Welcome to the Cisco TelePresence MCU 4505, version 4.3(2.18)\\r\\n
10.11.12.199	switch.test.com	80	HTTP	Networking	\\n \\n ProCurve Switch 2810-48G (J9022A)\\n
10.11.12.7	rcp.ne.test.com	8080	HTTP	-	404 Not Found
10.11.12.199	switch.test.com	23	TELNET	-	\\\\r\\\\nSorry, the maximum number of telnet sessions are active. Try again later.\\\\r\\\\n\\\\x00

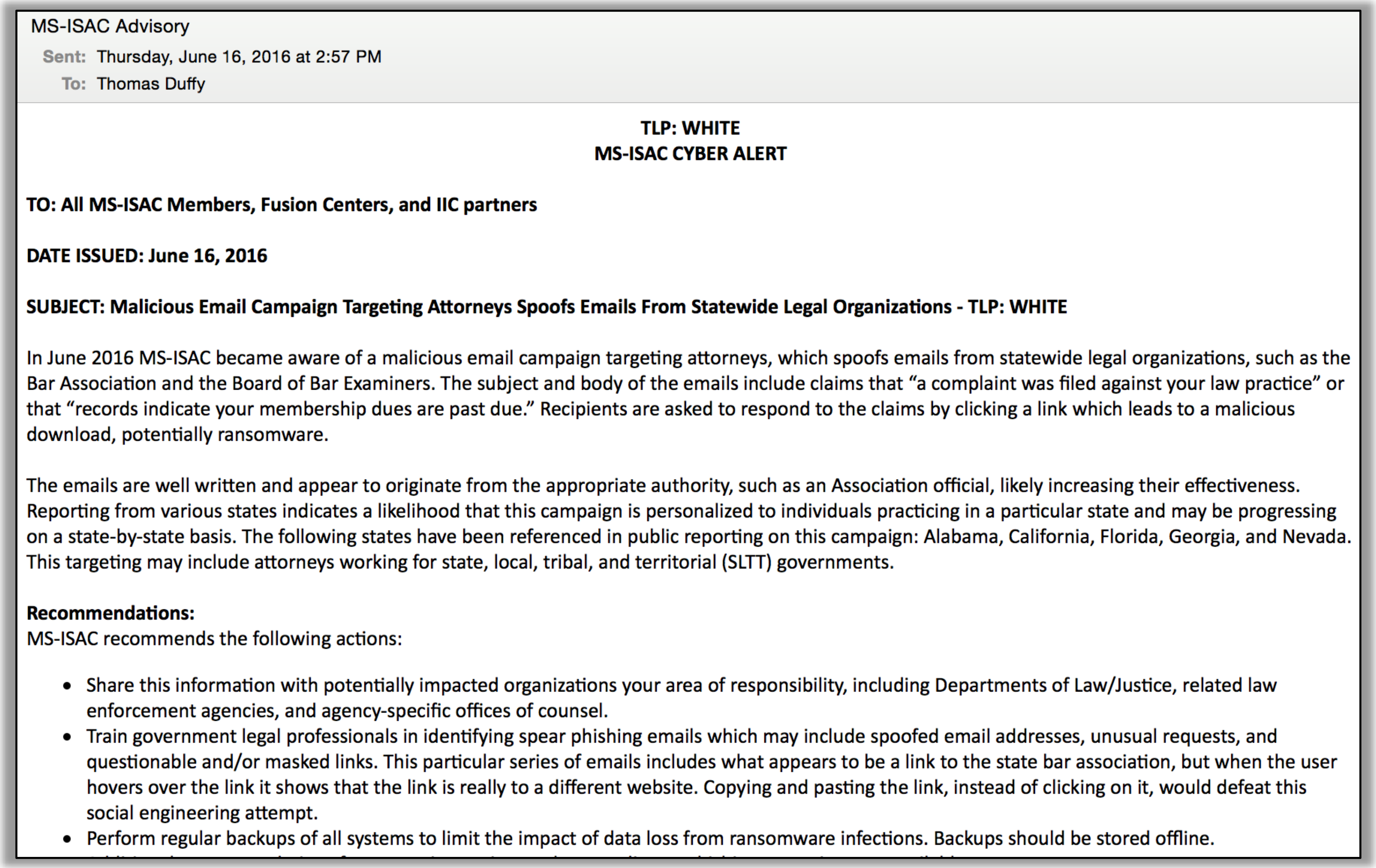
Malicious Code Analysis Platform

A web based service that enables members to submit and analyze suspicious files in a controlled and non-public fashion

- Executables
- DLLs
- Documents
- Quarantine files
- Archives

To gain an account contact:
mcap@cisecurity.org

MS-ISAC Cyber Alerts



MS-ISAC Advisory

Sent: Thursday, June 16, 2016 at 2:57 PM

To: Thomas Duffy

TLP: WHITE
MS-ISAC CYBER ALERT

TO: All MS-ISAC Members, Fusion Centers, and IIC partners

DATE ISSUED: June 16, 2016

SUBJECT: Malicious Email Campaign Targeting Attorneys Spoofs Emails From Statewide Legal Organizations - TLP: WHITE

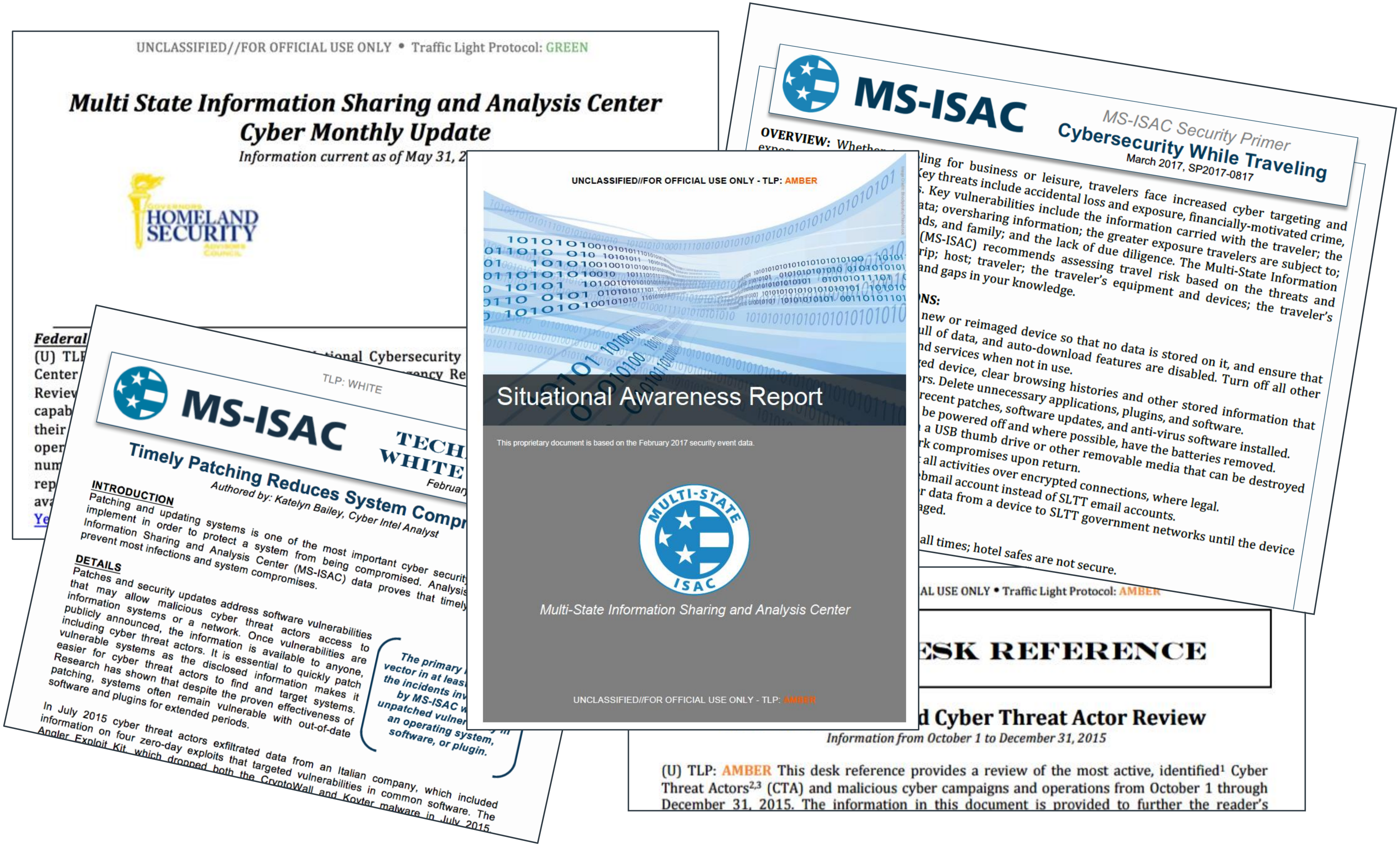
In June 2016 MS-ISAC became aware of a malicious email campaign targeting attorneys, which spoofs emails from statewide legal organizations, such as the Bar Association and the Board of Bar Examiners. The subject and body of the emails include claims that “a complaint was filed against your law practice” or that “records indicate your membership dues are past due.” Recipients are asked to respond to the claims by clicking a link which leads to a malicious download, potentially ransomware.

The emails are well written and appear to originate from the appropriate authority, such as an Association official, likely increasing their effectiveness. Reporting from various states indicates a likelihood that this campaign is personalized to individuals practicing in a particular state and may be progressing on a state-by-state basis. The following states have been referenced in public reporting on this campaign: Alabama, California, Florida, Georgia, and Nevada. This targeting may include attorneys working for state, local, tribal, and territorial (SLTT) governments.

Recommendations:
MS-ISAC recommends the following actions:

- Share this information with potentially impacted organizations your area of responsibility, including Departments of Law/Justice, related law enforcement agencies, and agency-specific offices of counsel.
- Train government legal professionals in identifying spear phishing emails which may include spoofed email addresses, unusual requests, and questionable and/or masked links. This particular series of emails includes what appears to be a link to the state bar association, but when the user hovers over the link it shows that the link is really to a different website. Copying and pasting the link, instead of clicking on it, would defeat this social engineering attempt.
- Perform regular backups of all systems to limit the impact of data loss from ransomware infections. Backups should be stored offline.

MS-ISAC Intel Papers



UNCLASSIFIED//FOR OFFICIAL USE ONLY • Traffic Light Protocol: GREEN

Multi State Information Sharing and Analysis Center
Cyber Monthly Update
Information current as of May 31, 2

Federal
(U) TLP ational Cybersecurity
Center gency Re
Review
capab
their
oper
num
rep
ava
Ye

TLP: WHITE

MS-ISAC

TECH
WHITE
Februar

Timely Patching Reduces System Compr

Authored by: Katelyn Bailey, Cyber Intel Analyst

INTRODUCTION
Patching and updating systems is one of the most important cyber securit implement in order to protect a system from being compromised. Analysis Information Sharing and Analysis Center (MS-ISAC) data proves that timely prevent most infections and system compromises.

DETAILS
Patches and security updates address software vulnerabilities that may allow malicious cyber threat actors access to information systems or a network. Once vulnerabilities are publicly announced, the information is available to anyone, including cyber threat actors. It is essential to quickly patch vulnerable systems as the disclosed information makes it easier for cyber threat actors to find and target systems. Research has shown that despite the proven effectiveness of patching, systems often remain vulnerable with out-of-date software and plugins for extended periods.

The primary vector in at leas the incidents inv by MS-ISAC w unpatched vulner an operating system, software, or plugin.

In July 2015 cyber threat actors exfiltrated data from an Italian company, which included information on four zero-day exploits that targeted vulnerabilities in common software. The Angler Exploit Kit, which dropped both the CryptoWall and Kovter malware in July 2015

UNCLASSIFIED//FOR OFFICIAL USE ONLY - TLP: AMBER

Situational Awareness Report

This proprietary document is based on the February 2017 security event data.

Multi-State Information Sharing and Analysis Center

UNCLASSIFIED//FOR OFFICIAL USE ONLY - TLP: AMBER

MS-ISAC

MS-ISAC Security Primer
Cybersecurity While Traveling
March 2017, SP2017-0817

OVERVIEW: Whether
expo ling for business or leisure, travelers face increased cyber targeting and Key threats include accidental loss and exposure, financially-motivated crime, s. Key vulnerabilities include the information carried with the traveler; the ata; oversharing information; the greater exposure travelers are subject to; nds, and family; and the lack of due diligence. The Multi-State Information (MS-ISAC) recommends assessing travel risk based on the threats and rip; host; traveler; the traveler's equipment and devices; the traveler's and gaps in your knowledge.

NS:
new or reimaged device so that no data is stored on it, and ensure that ull of data, and auto-download features are disabled. Turn off all other nd services when not in use.
ed device, clear browsing histories and other stored information that rs. Delete unnecessary applications, plugins, and software.
recent patches, software updates, and anti-virus software installed.
be powered off and where possible, have the batteries removed.
a USB thumb drive or other removable media that can be destroyed
rk compromises upon return.
all activities over encrypted connections, where legal.
bmail account instead of SLTT email accounts.
r data from a device to SLTT government networks until the device
aged.

all times; hotel safes are not secure.

AL USE ONLY • Traffic Light Protocol: AMBER

ESK REFERENCE

d Cyber Threat Actor Review
Information from October 1 to December 31, 2015

(U) TLP: AMBER This desk reference provides a review of the most active, identified[1] Cyber Threat Actors[2,3] (CTA) and malicious cyber campaigns and operations from October 1 through December 31, 2015. The information in this document is provided to further the reader's

TLP: WHITE

Nationwide Cyber Security Review

NCSR

A voluntary self-assessment survey designed to evaluate cyber security management within SLTT governments

All states (and agencies within),
local government jurisdictions (and departments within),
tribal and territorial governments can participate.

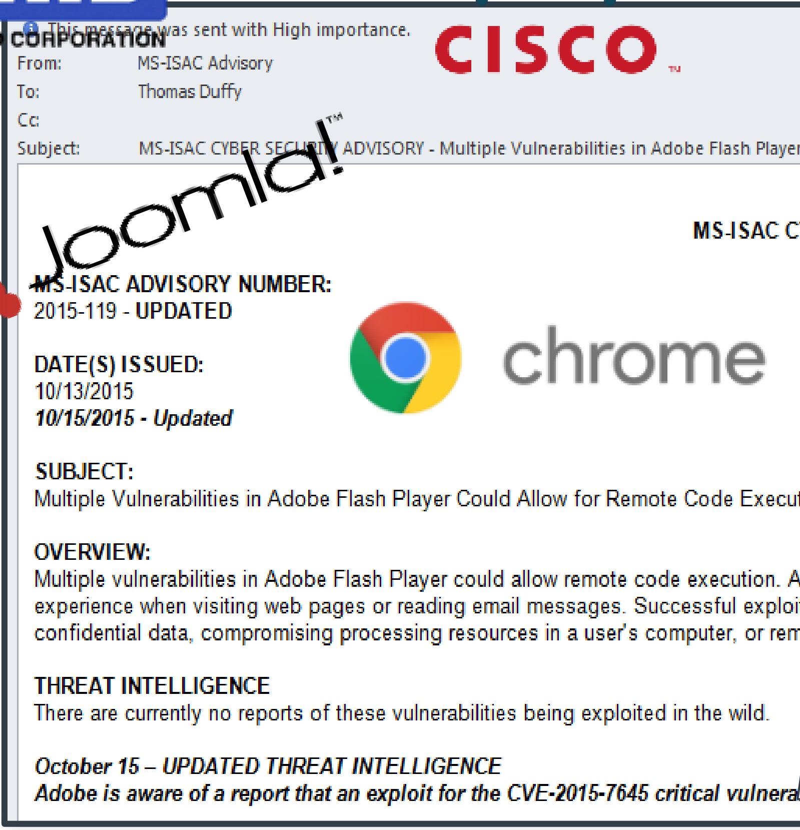
https://www.cisecurity.org/ms-isac/services/ncsr

CIS Center for Internet Security®

MS-ISAC Multi-State Information Sharing & Analysis Center

Resources for MS-ISAC Members and Private Organizations Too!

MS-ISAC Advisories



This message was sent with High importance.

From: MS-ISAC Advisory

To: Thomas Duffy

Cc:

Subject: MS-ISAC CYBER SECURITY ADVISORY - Multiple Vulnerabilities in Adobe Flash Player Could Allo

TLP: W

MS-ISAC CYBER S

MS-ISAC ADVISORY NUMBER:
2015-119 - UPDATED

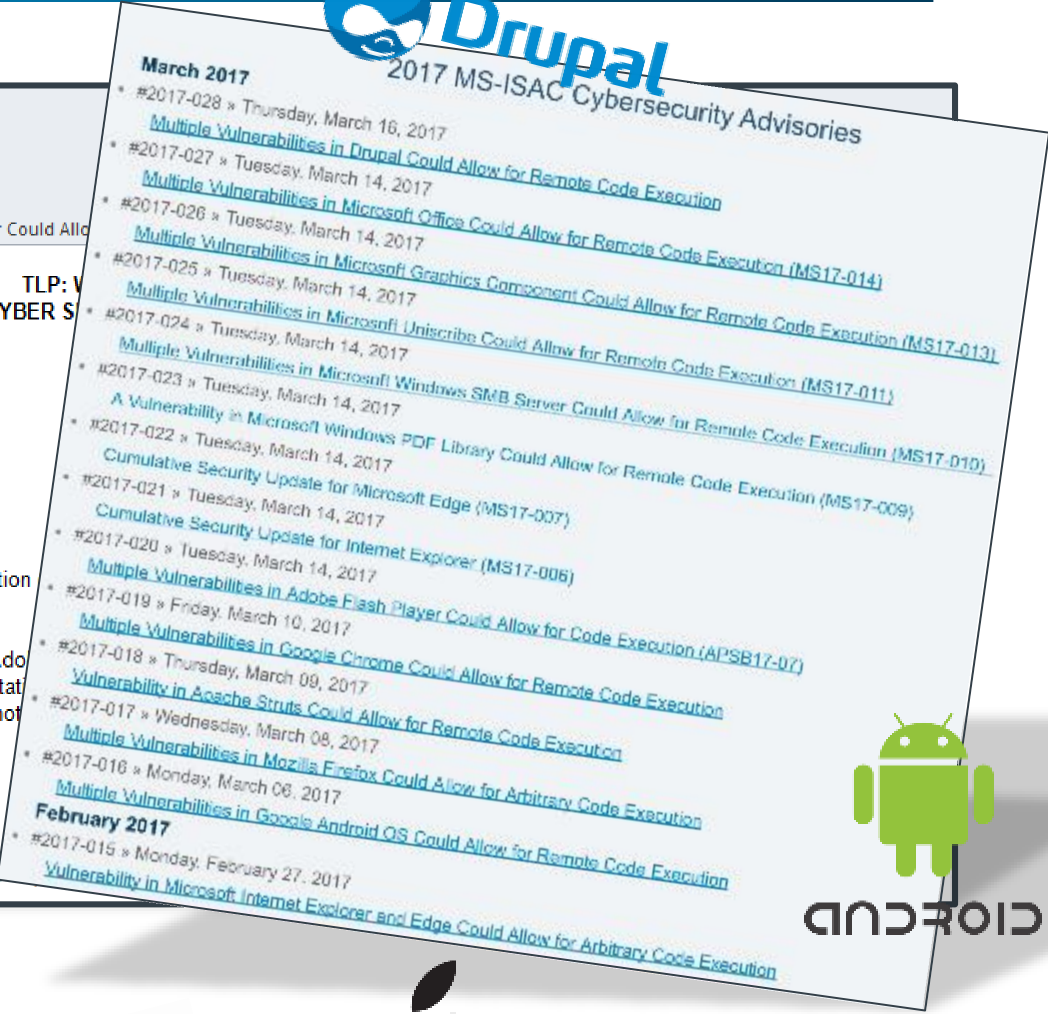
DATE(S) ISSUED:
10/13/2015
10/15/2015 - Updated

SUBJECT:
Multiple Vulnerabilities in Adobe Flash Player Could Allow for Remote Code Execution

OVERVIEW:
Multiple vulnerabilities in Adobe Flash Player could allow remote code execution. Ado experience when visiting web pages or reading email messages. Successful exploitat confidential data, compromising processing resources in a user's computer, or remot

THREAT INTELLIGENCE
There are currently no reports of these vulnerabilities being exploited in the wild.

October 15 – UPDATED THREAT INTELLIGENCE
Adobe is aware of a report that an exploit for the CVE-2015-7645 critical vulnera



2017 MS-ISAC Cybersecurity Advisories

March 2017

- #2017-028 » Thursday, March 16, 2017
  Multiple Vulnerabilities in Drupal Could Allow for Remote Code Execution
- #2017-027 » Tuesday, March 14, 2017
  Multiple Vulnerabilities in Microsoft Office Could Allow for Remote Code Execution (MS17-014)
- #2017-026 » Tuesday, March 14, 2017
  Multiple Vulnerabilities in Microsoft Graphics Component Could Allow for Remote Code Execution (MS17-013)
- #2017-025 » Tuesday, March 14, 2017
  Multiple Vulnerabilities in Microsoft Uniscribe Could Allow for Remote Code Execution (MS17-011)
- #2017-024 » Tuesday, March 14, 2017
  Multiple Vulnerabilities in Microsoft Windows SMB Server Could Allow for Remote Code Execution (MS17-010)
- #2017-023 » Tuesday, March 14, 2017
  A Vulnerability in Microsoft Windows PDF Library Could Allow for Remote Code Execution (MS17-009)
- #2017-022 » Tuesday, March 14, 2017
  Cumulative Security Update for Microsoft Edge (MS17-007)
- #2017-021 » Tuesday, March 14, 2017
  Cumulative Security Update for Internet Explorer (MS17-006)
- #2017-020 » Tuesday, March 14, 2017
  Multiple Vulnerabilities in Adobe Flash Player Could Allow for Code Execution (APSB17-07)
- #2017-019 » Friday, March 10, 2017
  Multiple Vulnerabilities in Google Chrome Could Allow for Remote Code Execution
- #2017-018 » Thursday, March 09, 2017
  Vulnerability in Apache Struts Could Allow for Remote Code Execution
- #2017-017 » Wednesday, March 08, 2017
  Multiple Vulnerabilities in Mozilla Firefox Could Allow for Arbitrary Code Execution
- #2017-016 » Monday, March 06, 2017
  Multiple Vulnerabilities in Google Android OS Could Allow for Remote Code Execution

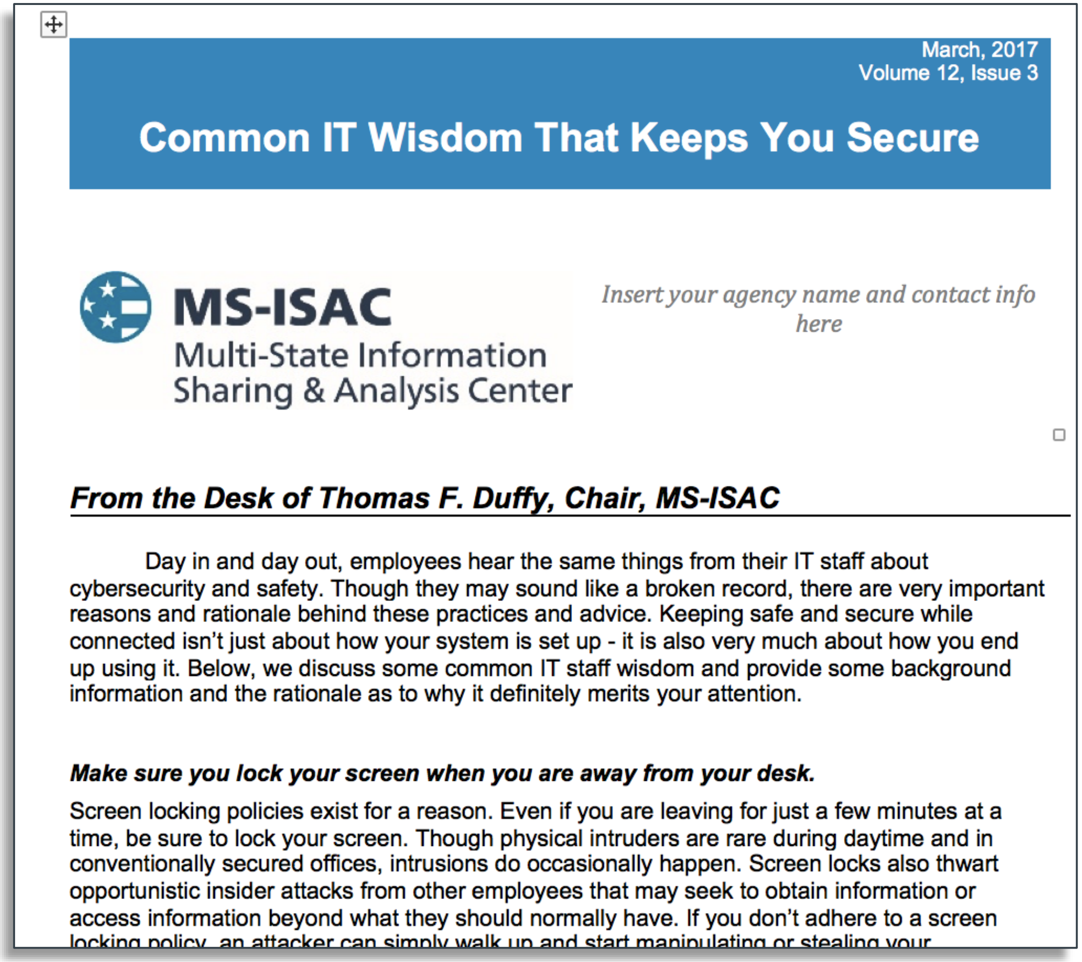
February 2017

- #2017-015 » Monday, February 27, 2017
  Vulnerability in Microsoft Internet Explorer and Edge Could Allow for Arbitrary Code Execution

TLP: WHITE

Monthly Newsletter

Distributed in template form to allow for
re-branding and redistribution by your agency



March, 2017
Volume 12, Issue 3

Common IT Wisdom That Keeps You Secure

MS-ISAC
Multi-State Information
Sharing & Analysis Center

Insert your agency name and contact info here

From the Desk of Thomas F. Duffy, Chair, MS-ISAC

Day in and day out, employees hear the same things from their IT staff about cybersecurity and safety. Though they may sound like a broken record, there are very important reasons and rationale behind these practices and advice. Keeping safe and secure while connected isn't just about how your system is set up - it is also very much about how you end up using it. Below, we discuss some common IT staff wisdom and provide some background information and the rationale as to why it definitely merits your attention.

Make sure you lock your screen when you are away from your desk.

Screen locking policies exist for a reason. Even if you are leaving for just a few minutes at a time, be sure to lock your screen. Though physical intruders are rare during daytime and in conventionally secured offices, intrusions do occasionally happen. Screen locks also thwart opportunistic insider attacks from other employees that may seek to obtain information or access information beyond what they should normally have. If you don't adhere to a screen locking policy, an attacker can simply walk up and start manipulating or stealing your

Stay Safe Online

Powered by the National Cyber Security Alliance Publishes:

- Tips Sheets
- Small Business Toolkit
- Secure Key Devices

PROTECT YOUR CUSTOMERS

CYBER-CEO INITIATIVE

GRADES K-2

THE COMMUNITY

TRAIN YOUR EMPLOYEES

GRADES 3-5

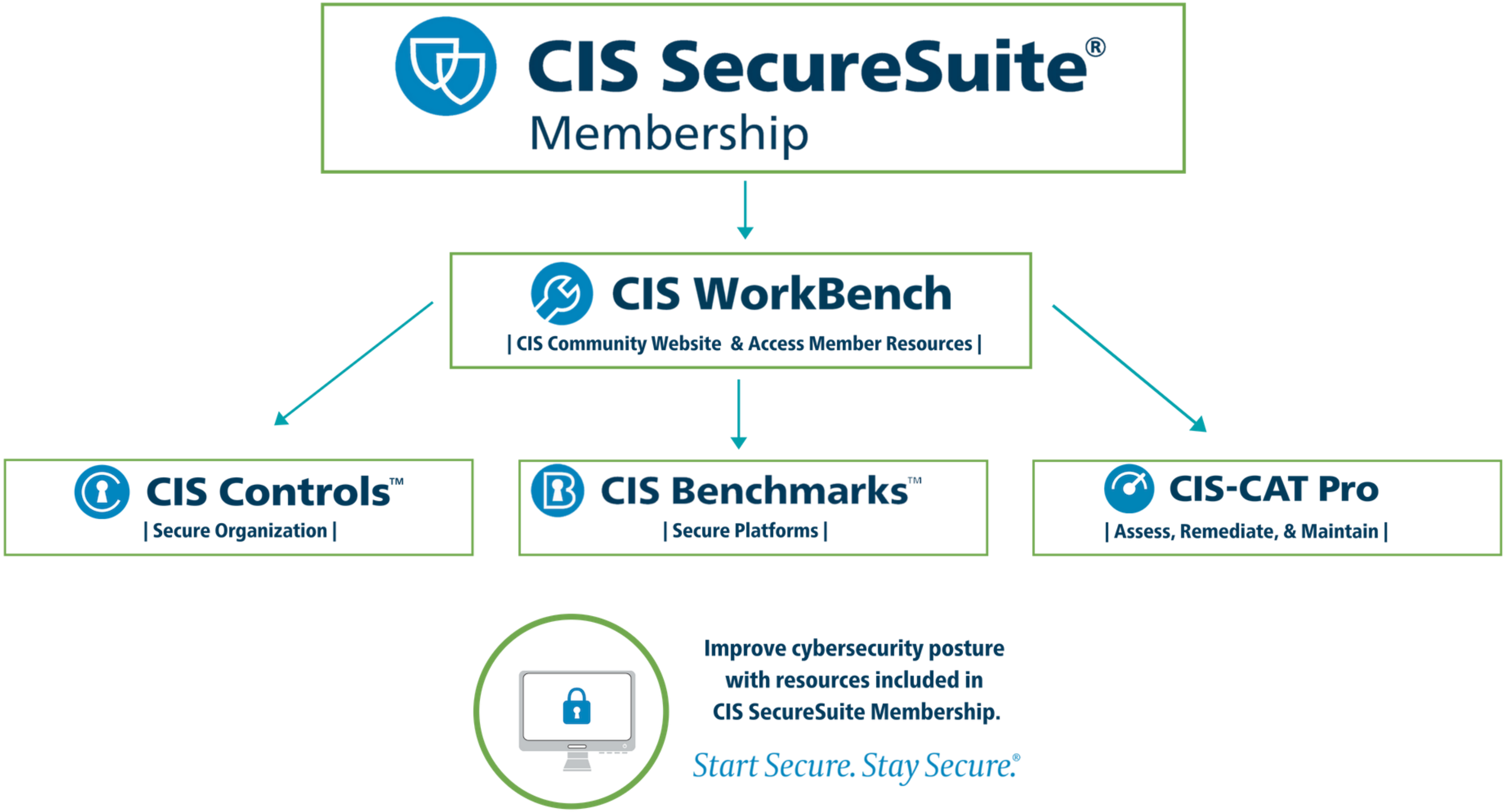
IMPLEMENT A CYBERSECURITY PLAN

MIDDLE & HIGH SCHOOL

HIGHER EDUCATION

www.staysafeonline.org

CIS SecureSuite



CIS SecureSuite® Membership

CIS WorkBench

| CIS Community Website & Access Member Resources |

CIS Controls™

| Secure Organization |

CIS Benchmarks™

| Secure Platforms |

CIS-CAT Pro

| Assess, Remediate, & Maintain |

Improve cybersecurity posture with resources included in CIS SecureSuite Membership.

Start Secure. Stay Secure.®

Who do I call?

Security Operations Center (SOC)

SOC@cisecurity.org - 1-866-787-4722

31 Tech Valley Dr., East Greenbush, NY 12061-4134

www.cisecurity.org

to join or get more information:

https://learn.cisecurity.org/ms-isac-registration

TLP: WHITE

CIS™ Center for Internet Security®

MS-ISAC
Multi-State Information
Sharing & Analysis Center

MS-ISAC 24x7 Security Operations Center

1-866-787-4722

SOC@cisecurity.org

info@cisecurity.org

Greta Noble
Senior Program Specialist
MS-ISAC
518.880.0740
Greta.noble@cisecurity.org

Brendan Montagne
Program Specialist
MS-ISAC
518.880.0689
Brendan.montagne@cisecurity.org