American Hospital Association®

The COVID Cyber and Privacy Threat Landscape

CONFIDENTIALITY COALITION

Advancing Health Care. Safeguarding Trust.

Presented by John Riggi, Senior Advisor, Cybersecurity and Risk Advisory Services 6/18/2020

American Hospital Association™

Advancing Health in America

AHA CENTER FOR HEALTH INNOVATION

Agenda

- ➢ COVID-19 Cyber Threats Update
- ➢ Cyber Attack Methodology
- ➢ Cyber and Privacy Policy Issues + Resources

Corona Virus and Cyber Viruses: Cyber Criminals Exploiting a Crisis

Ventilators and Life Support Devices

Phishing Emails

Telehealth and Telework vulnerabilities

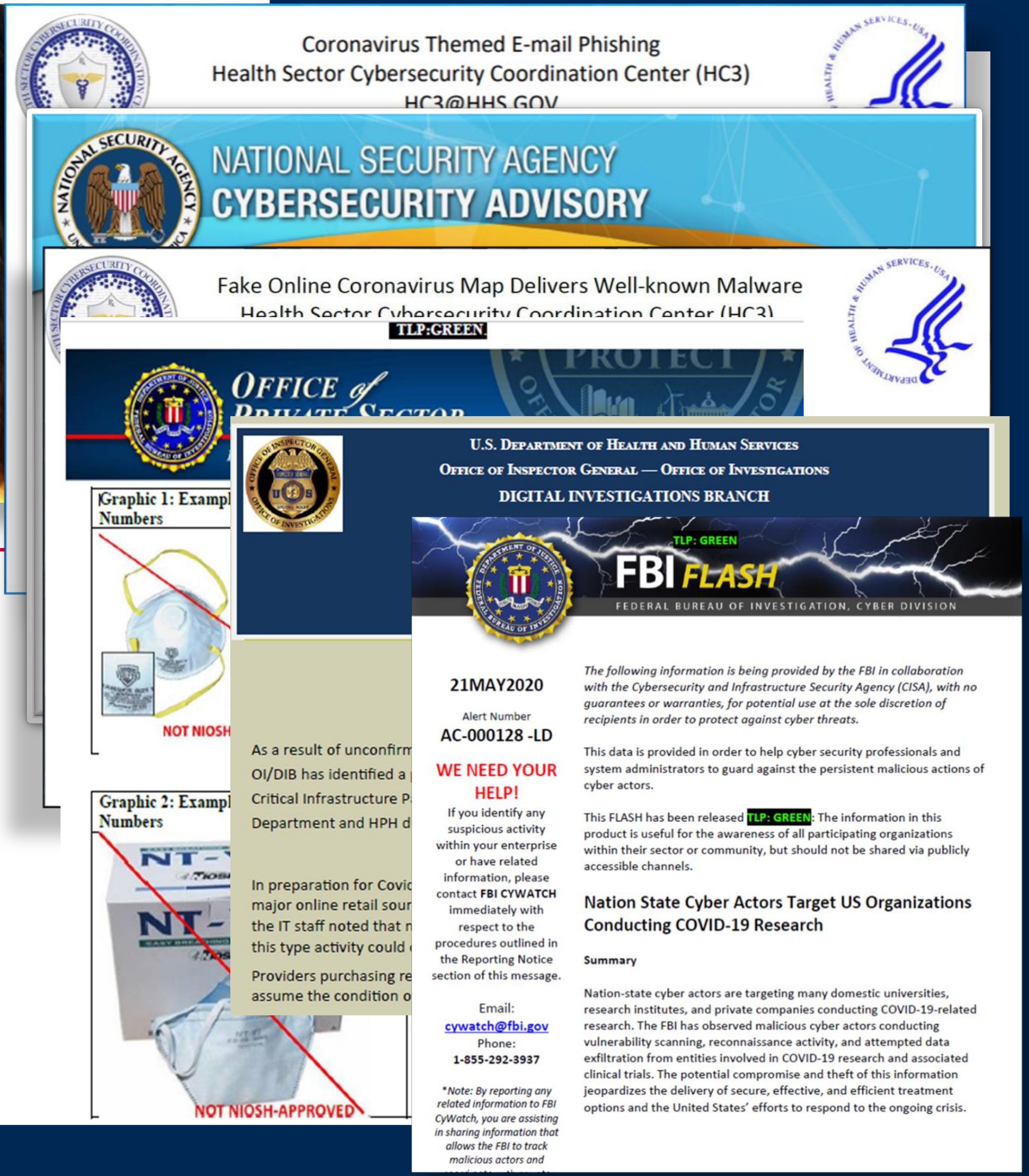
Cloud Vulnerabilities

Malicious Sites

Online Fraudulent PPE Schemes

Supple Chain Risk

Theft of research on treatments and vaccine



Coronavirus Themed E-mail Phishing
Health Sector Cybersecurity Coordination Center (HC3)
HC3@HHS.GOV

NATIONAL SECURITY AGENCY
CYBERSECURITY ADVISORY

Fake Online Coronavirus Map Delivers Well-known Malware
Health Sector Cybersecurity Coordination Center (HC3)

TLP:GREEN

OFFICE of PRIVATE SECTOR

Graphic 1: Exampl
Numbers

NOT NIOSH

Graphic 2: Exampl
Numbers

NOT NIOSH-APPROVED

U.S. Department of Health and Human Services
Office of Inspector General — Office of Investigations
DIGITAL INVESTIGATIONS BRANCH

As a result of unconfirm
OI/DIB has identified a
Critical Infrastructure P
Department and HPH d

In preparation for Covic
major online retail sour
the IT staff noted that r
this type activity could
Providers purchasing re
assume the condition o

TLP: GREEN

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

21MAY2020

Alert Number
AC-000128 -LD

WE NEED YOUR HELP!

If you identify any suspicious activity within your enterprise or have related information, please contact FBI CYWATCH immediately with respect to the procedures outlined in the Reporting Notice section of this message.

Email:
cywatch@fbi.gov
Phone:
1-855-292-3937

*Note: By reporting any related information to FBI CyWatch, you are assisting in sharing information that allows the FBI to track malicious actors and

The following information is being provided by the FBI in collaboration with the Cybersecurity and Infrastructure Security Agency (CISA), with no guarantees or warranties, for potential use at the sole discretion of recipients in order to protect against cyber threats.

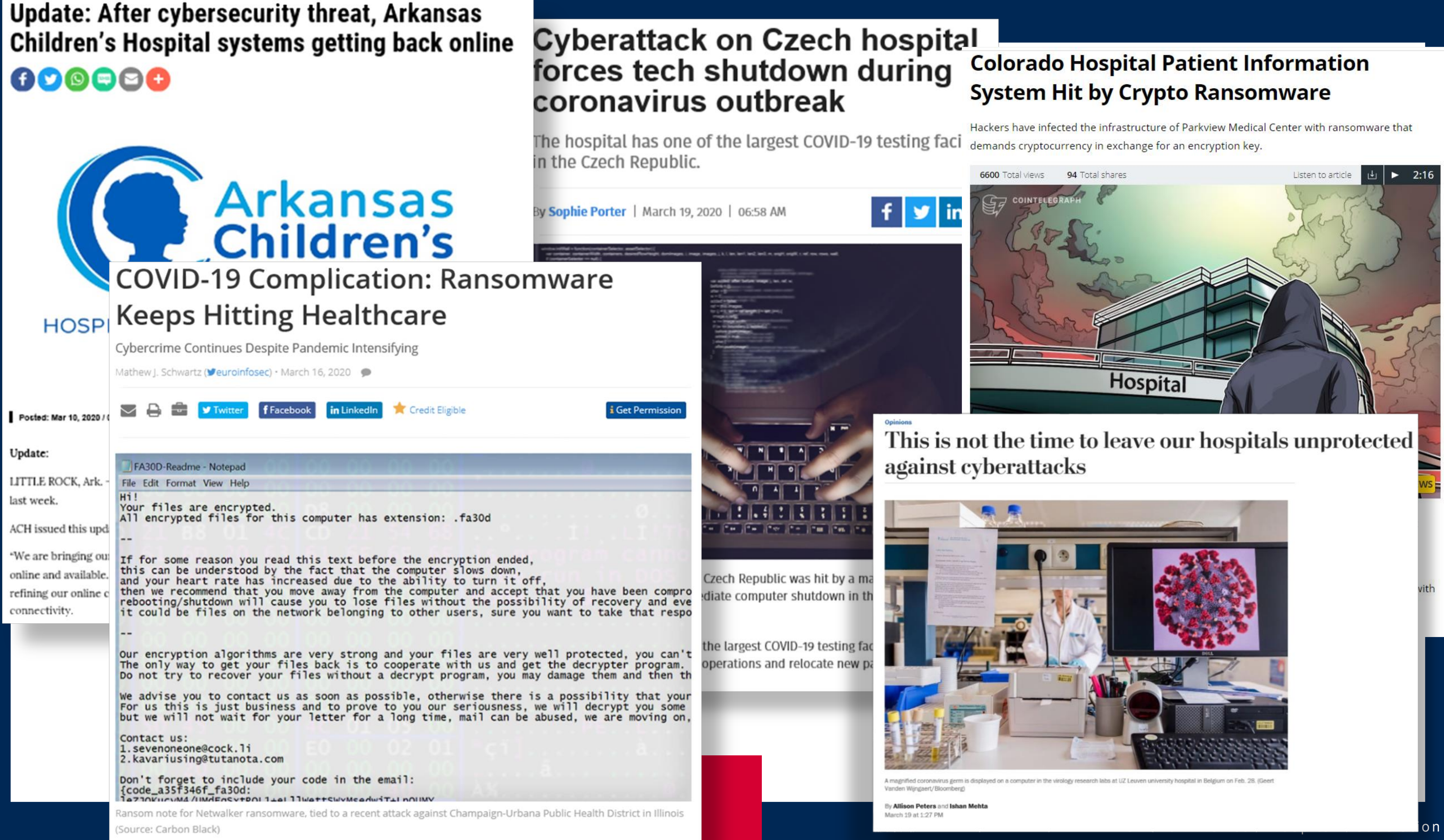
This data is provided in order to help cyber security professionals and system administrators to guard against the persistent malicious actions of cyber actors.

This FLASH has been released TLP: GREEN: The information in this product is useful for the awareness of all participating organizations within their sector or community, but should not be shared via publicly accessible channels.

Nation State Cyber Actors Target US Organizations Conducting COVID-19 Research

Summary

Nation-state cyber actors are targeting many domestic universities, research institutes, and private companies conducting COVID-19-related research. The FBI has observed malicious cyber actors conducting vulnerability scanning, reconnaissance activity, and attempted data exfiltration from entities involved in COVID-19 research and associated clinical trials. The potential compromise and theft of this information jeopardizes the delivery of secure, effective, and efficient treatment options and the United States' efforts to respond to the ongoing crisis.



Update: After cybersecurity threat, Arkansas Children's Hospital systems getting back online

Posted: Mar 10, 2020 / (

Update:

LITTLE ROCK, Ark. -
last week.

ACH issued this upd

"We are bringing ou
online and available.
refining our online c
connectivity.

Cyberattack on Czech hospital forces tech shutdown during coronavirus outbreak

The hospital has one of the largest COVID-19 testing faci
in the Czech Republic.

By Sophie Porter | March 19, 2020 | 06:58 AM

Czech Republic was hit by a ma
ediate computer shutdown in th

the largest COVID-19 testing fac
operations and relocate new pa

Colorado Hospital Patient Information System Hit by Crypto Ransomware

Hackers have infected the infrastructure of Parkview Medical Center with ransomware that demands cryptocurrency in exchange for an encryption key.

6600 Total views 94 Total shares Listen to article 2:16

COVID-19 Complication: Ransomware Keeps Hitting Healthcare

Cybercrime Continues Despite Pandemic Intensifying

Mathew J. Schwartz (euroinfosec) • March 16, 2020

FA30D-Readme - Notepad

```
Hi!
Your files are encrypted.
All encrypted files for this computer has extension: .fa30d

--

If for some reason you read this text before the encryption ended,
this can be understood by the fact that the computer slows down,
and your heart rate has increased due to the ability to turn it off,
then we recommend that you move away from the computer and accept that you have been compro
rebooting/shutdown will cause you to lose files without the possibility of recovery and eve
it could be files on the network belonging to other users, sure you want to take that respo

--

Our encryption algorithms are very strong and your files are very well protected, you can't
The only way to get your files back is to cooperate with us and get the decrypter program.
Do not try to recover your files without a decrypt program, you may damage them and then th

We advise you to contact us as soon as possible, otherwise there is a possibility that your
For us this is just business and to prove to you our seriousness, we will decrypt you some
but we will not wait for your letter for a long time, mail can be abused, we are moving on,

Contact us:
1.sevenoneone@cock.li
2.kavariusing@tutanota.com

Don't forget to include your code in the email:
{code_a35f346f_fa30d:
1eZJOKucvM4/UMdEqSxtROL1+eLl1WettSWxMsedwiT+LpOUMX
```

Ransom note for Netwalker ransomware, tied to a recent attack against Champaign-Urbana Public Health District in Illinois (Source: Carbon Black)

Opinions

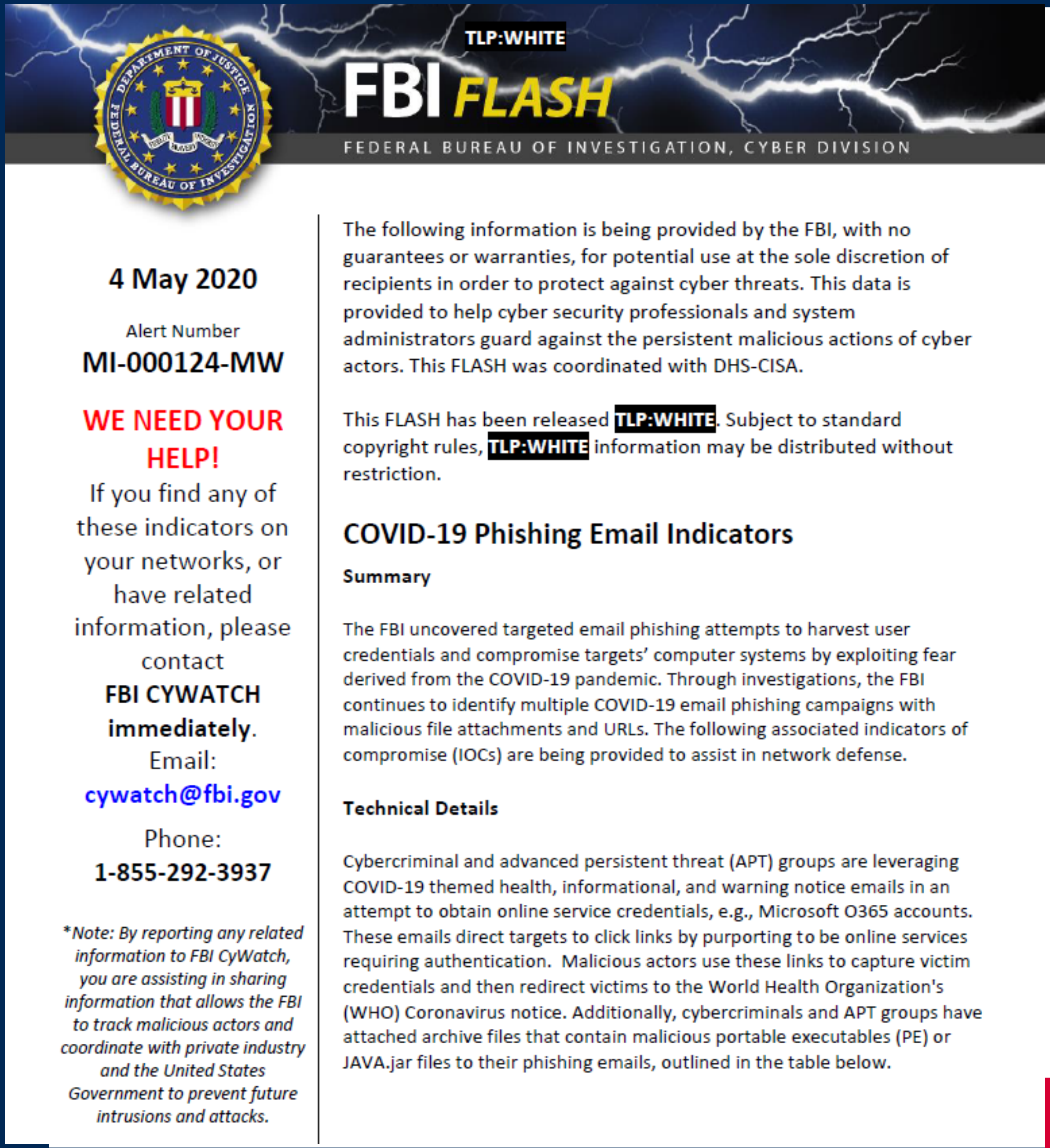
This is not the time to leave our hospitals unprotected against cyberattacks

A magnified coronavirus germ is displayed on a computer in the virology research labs at UZ Leuven university hospital in Belgium on Feb. 28. (Geert Vanden Wijngaert/Bloomberg)

By **Allison Peters** and **Ishan Mehta**
March 19 at 1:27 PM

“A ransomware attack on a hospital is a not just an economic crime, it’s a threat to life crime…and it should be prioritized, pursued and prosecuted as such ”

John Riggi, AHA Senior for Cybersecurity and Risk



TLP:WHITE

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

4 May 2020

Alert Number

MI-000124-MW

WE NEED YOUR HELP!

If you find any of these indicators on your networks, or have related information, please contact

FBI CYWATCH immediately.

Email:

cywatch@fbi.gov

Phone:

1-855-292-3937

**Note: By reporting any related information to FBI CyWatch, you are assisting in sharing information that allows the FBI to track malicious actors and coordinate with private industry and the United States Government to prevent future intrusions and attacks.*

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients in order to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors. This FLASH was coordinated with DHS-CISA.

This FLASH has been released **TLP:WHITE**. Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction.

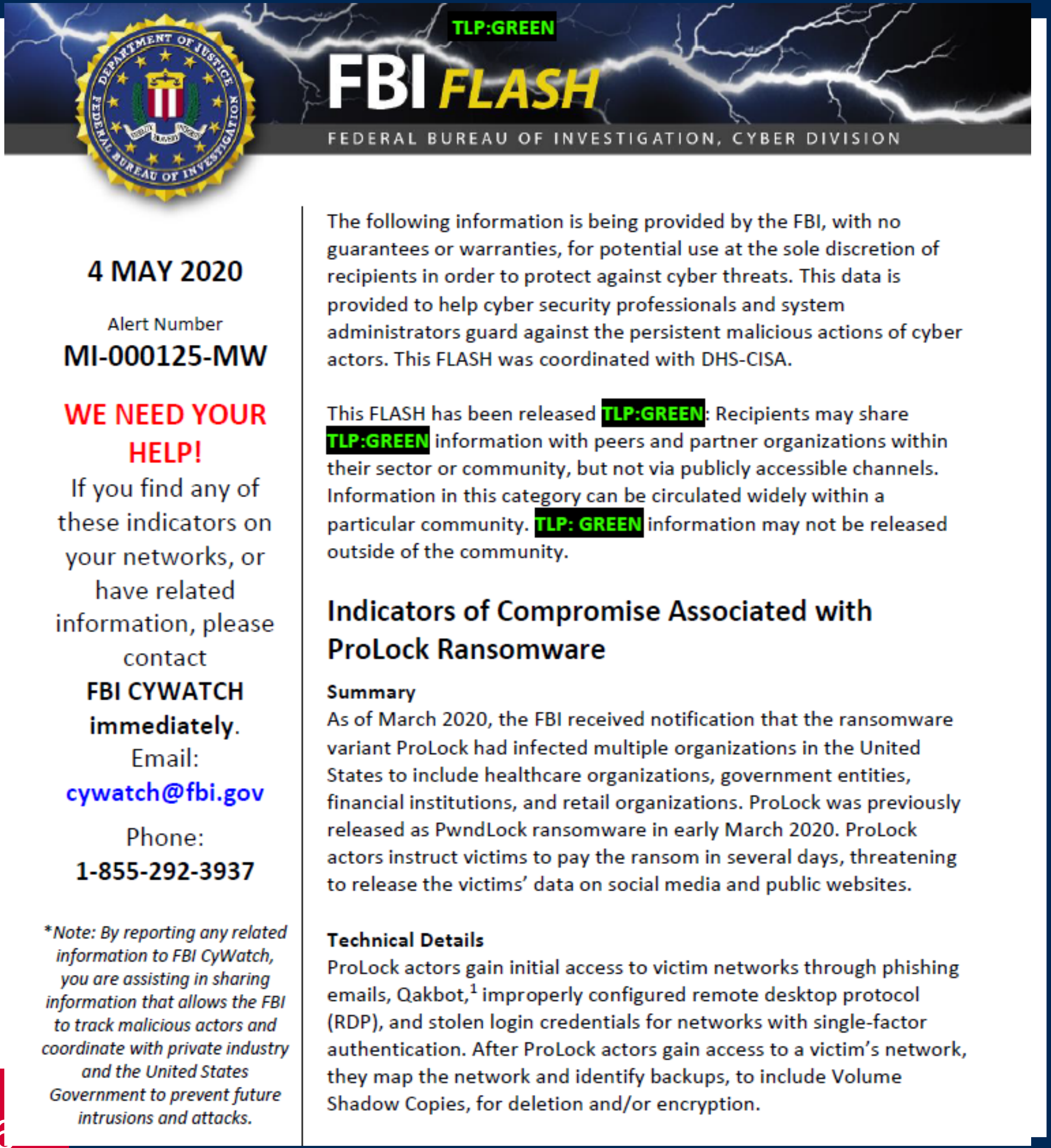
COVID-19 Phishing Email Indicators

Summary

The FBI uncovered targeted email phishing attempts to harvest user credentials and compromise targets' computer systems by exploiting fear derived from the COVID-19 pandemic. Through investigations, the FBI continues to identify multiple COVID-19 email phishing campaigns with malicious file attachments and URLs. The following associated indicators of compromise (IOCs) are being provided to assist in network defense.

Technical Details

Cybercriminal and advanced persistent threat (APT) groups are leveraging COVID-19 themed health, informational, and warning notice emails in an attempt to obtain online service credentials, e.g., Microsoft O365 accounts. These emails direct targets to click links by purporting to be online services requiring authentication. Malicious actors use these links to capture victim credentials and then redirect victims to the World Health Organization's (WHO) Coronavirus notice. Additionally, cybercriminals and APT groups have attached archive files that contain malicious portable executables (PE) or JAVA.jar files to their phishing emails, outlined in the table below.



TLP:GREEN

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

4 MAY 2020

Alert Number

MI-000125-MW

WE NEED YOUR HELP!

If you find any of these indicators on your networks, or have related information, please contact

FBI CYWATCH immediately.

Email:

cywatch@fbi.gov

Phone:

1-855-292-3937

**Note: By reporting any related information to FBI CyWatch, you are assisting in sharing information that allows the FBI to track malicious actors and coordinate with private industry and the United States Government to prevent future intrusions and attacks.*

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients in order to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors. This FLASH was coordinated with DHS-CISA.

This FLASH has been released **TLP:GREEN**: Recipients may share **TLP:GREEN** information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. **TLP: GREEN** information may not be released outside of the community.

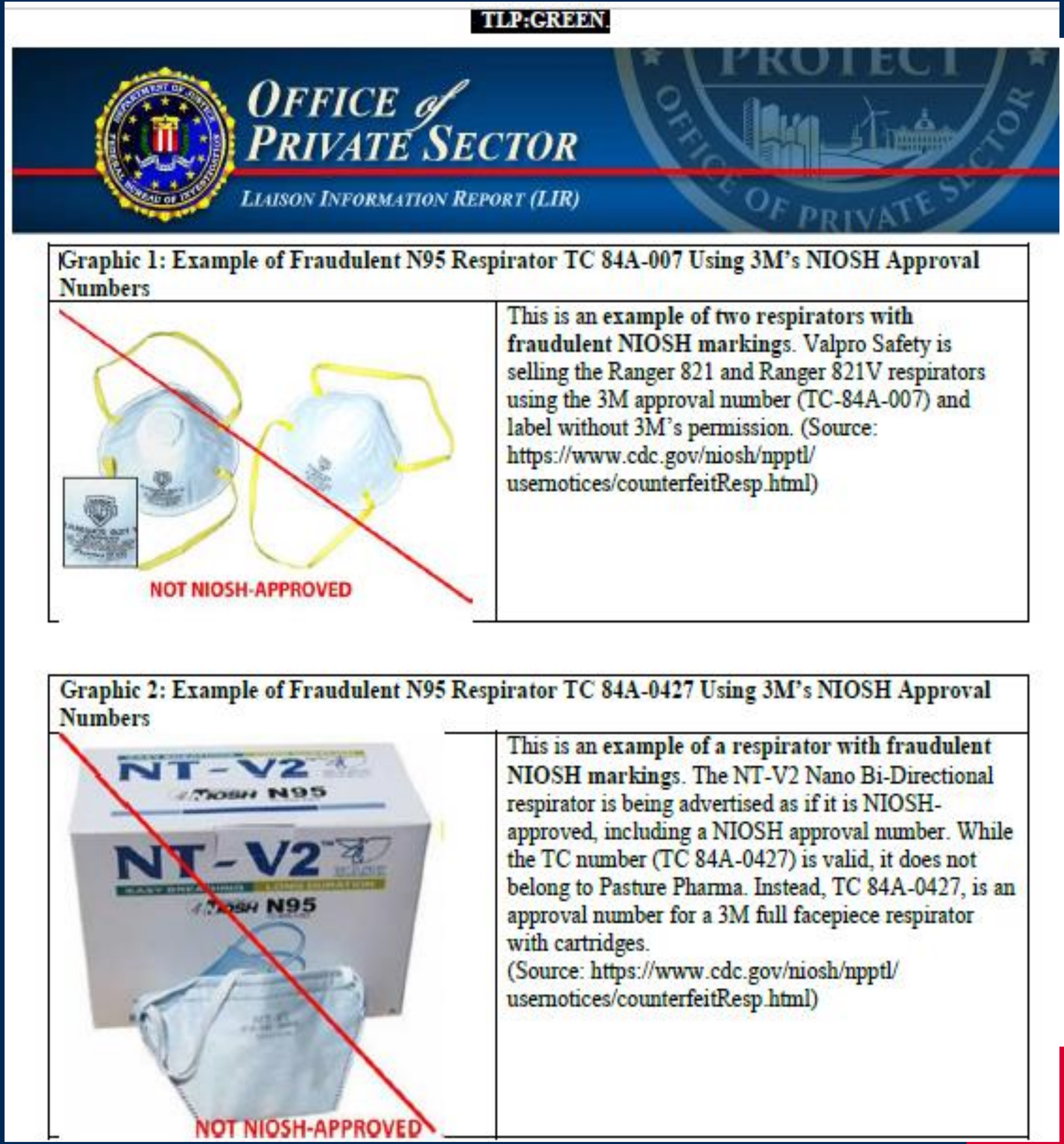
Indicators of Compromise Associated with ProLock Ransomware

Summary

As of March 2020, the FBI received notification that the ransomware variant ProLock had infected multiple organizations in the United States to include healthcare organizations, government entities, financial institutions, and retail organizations. ProLock was previously released as PwndLock ransomware in early March 2020. ProLock actors instruct victims to pay the ransom in several days, threatening to release the victims' data on social media and public websites.

Technical Details

ProLock actors gain initial access to victim networks through phishing emails, Qakbot,[1] improperly configured remote desktop protocol (RDP), and stolen login credentials for networks with single-factor authentication. After ProLock actors gain access to a victim's network, they map the network and identify backups, to include Volume Shadow Copies, for deletion and/or encryption.



TLP:GREEN

OFFICE of PRIVATE SECTOR

LIAISON INFORMATION REPORT (LIR)

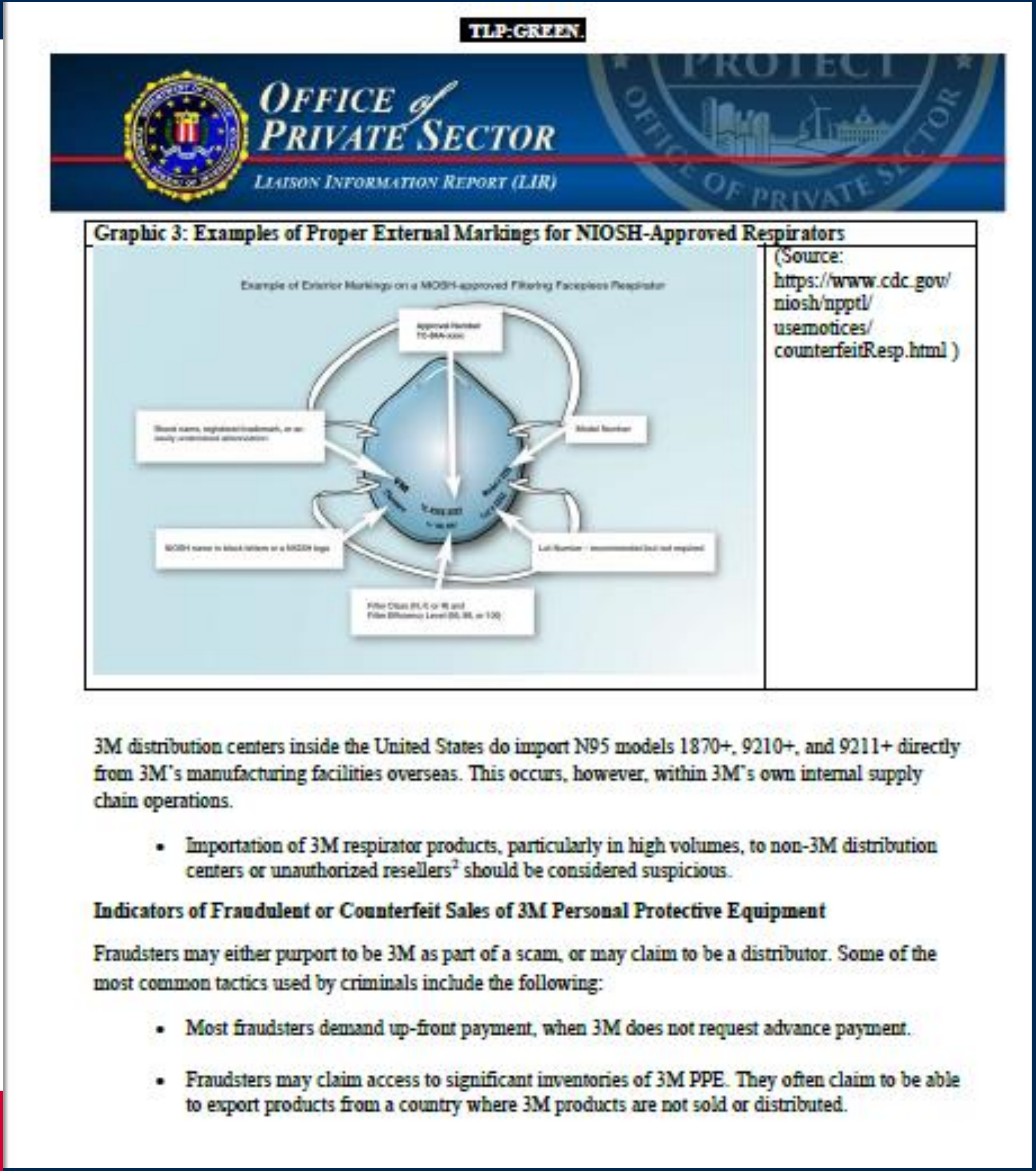
Graphic 1: Example of Fraudulent N95 Respirator TC 84A-007 Using 3M's NIOSH Approval Numbers

NOT NIOSH-APPROVED

This is an **example of two respirators with fraudulent NIOSH markings**. Valpro Safety is selling the Ranger 821 and Ranger 821V respirators using the 3M approval number (TC-84A-007) and label without 3M's permission. (Source: https://www.cdc.gov/niosh/npptl/usernotices/counterfeitResp.html)

Graphic 2: Example of Fraudulent N95 Respirator TC 84A-0427 Using 3M's NIOSH Approval Numbers

This is an **example of a respirator with fraudulent NIOSH markings**. The NT-V2 Nano Bi-Directional respirator is being advertised as if it is NIOSH-approved, including a NIOSH approval number. While the TC number (TC 84A-0427) is valid, it does not belong to Pasture Pharma. Instead, TC 84A-0427, is an approval number for a 3M full facepiece respirator with cartridges.
(Source: https://www.cdc.gov/niosh/npptl/usernotices/counterfeitResp.html)



TLP:GREEN

OFFICE of PRIVATE SECTOR

LIAISON INFORMATION REPORT (LIR)

Graphic 3: Examples of Proper External Markings for NIOSH-Approved Respirators

Example of Exterior Markings on a NIOSH-approved Filtering Facepiece Respirator
Approval Number TC-84A-xxxx
Brand name, registered trademark, or an easily understood abbreviation
Model Number
NIOSH name in block letters or a NIOSH logo
Lot Number – recommended but not required
Filter Class (N, R, or P) and Filter Efficiency Level (95, 99, or 100)

(Source: https://www.cdc.gov/niosh/npptl/usernotices/counterfeitResp.html)

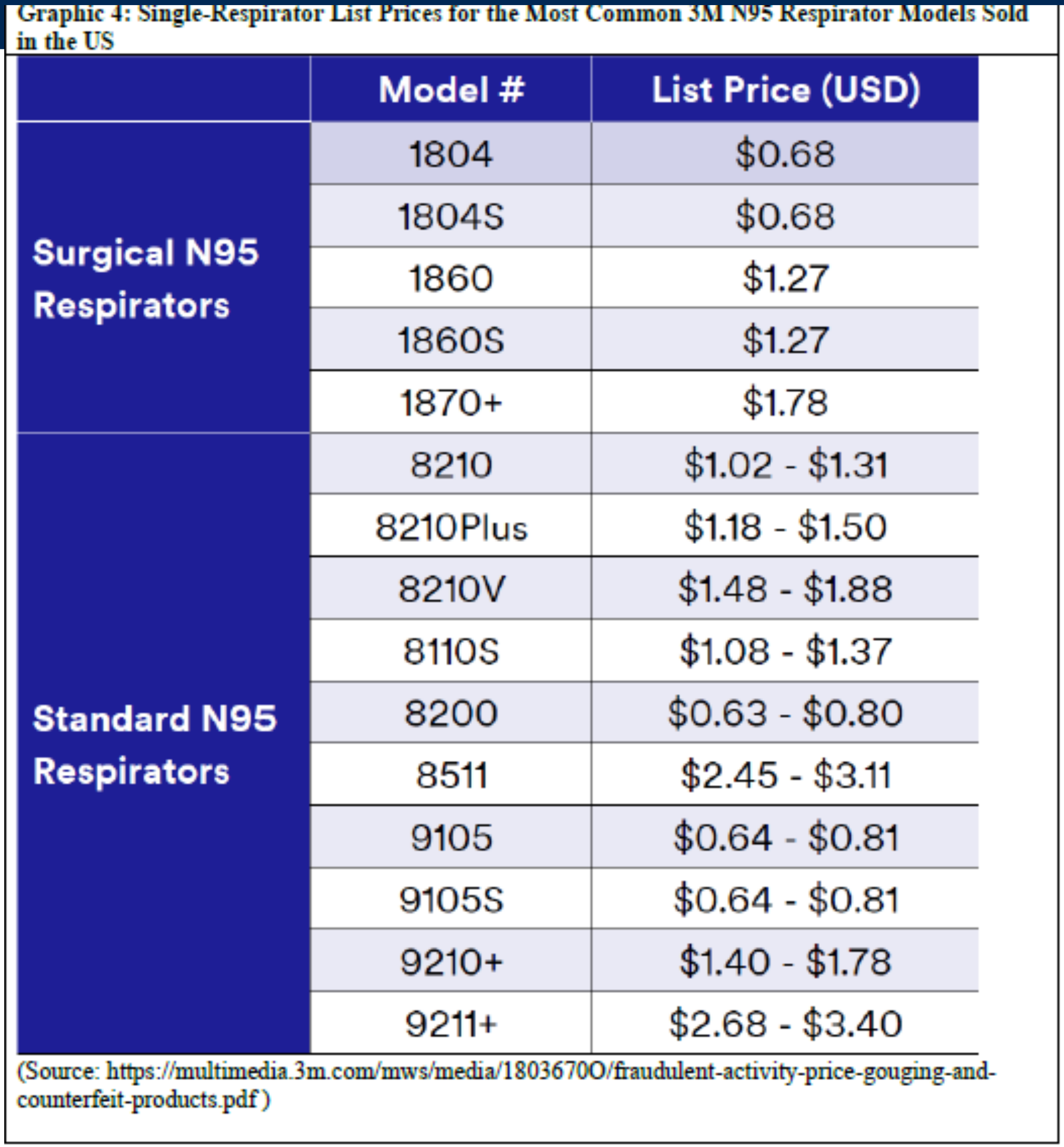
3M distribution centers inside the United States do import N95 models 1870+, 9210+, and 9211+ directly from 3M's manufacturing facilities overseas. This occurs, however, within 3M's own internal supply chain operations.

- Importation of 3M respirator products, particularly in high volumes, to non-3M distribution centers or unauthorized resellers[2] should be considered suspicious.

Indicators of Fraudulent or Counterfeit Sales of 3M Personal Protective Equipment

Fraudsters may either purport to be 3M as part of a scam, or may claim to be a distributor. Some of the most common tactics used by criminals include the following:

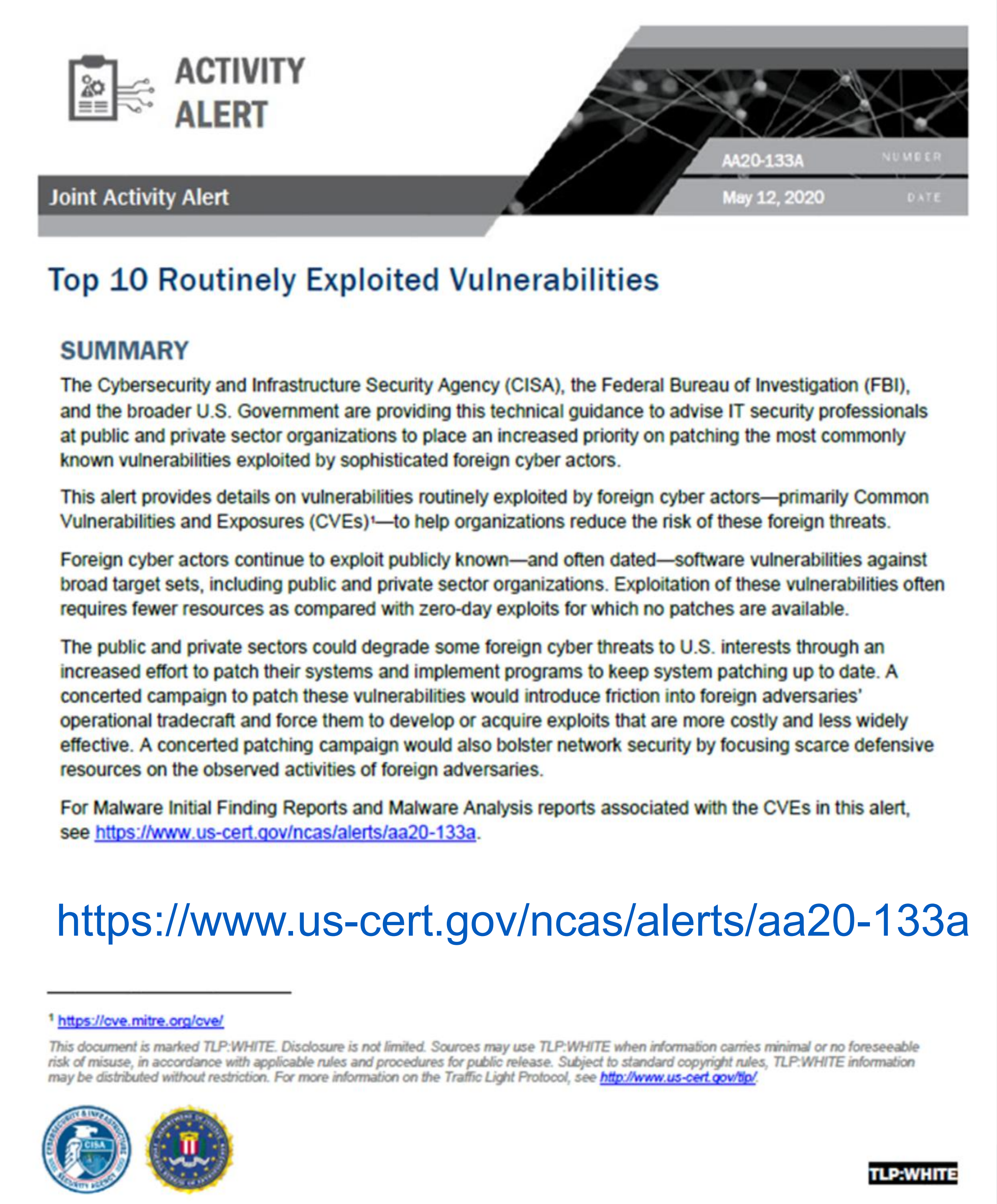
- Most fraudsters demand up-front payment, when 3M does not request advance payment.
- Fraudsters may claim access to significant inventories of 3M PPE. They often claim to be able to export products from a country where 3M products are not sold or distributed.



Graphic 4: Single-Respirator List Prices for the Most Common 3M N95 Respirator Models Sold in the US

	Model #	List Price (USD)
Surgical N95 Respirators	1804	$0.68
	1804S	$0.68
	1860	$1.27
	1860S	$1.27
	1870+	$1.78
Standard N95 Respirators	8210	$1.02 - $1.31
	8210Plus	$1.18 - $1.50
	8210V	$1.48 - $1.88
	8110S	$1.08 - $1.37
	8200	$0.63 - $0.80
	8511	$2.45 - $3.11
	9105	$0.64 - $0.81
	9105S	$0.64 - $0.81
	9210+	$1.40 - $1.78
	9211+	$2.68 - $3.40

(Source: https://multimedia.3m.com/mws/media/1803670O/fraudulent-activity-price-gouging-and-counterfeit-products.pdf)



ACTIVITY ALERT

Joint Activity Alert

AA20-133A NUMBER

May 12, 2020 DATE

Top 10 Routinely Exploited Vulnerabilities

SUMMARY

The Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the broader U.S. Government are providing this technical guidance to advise IT security professionals at public and private sector organizations to place an increased priority on patching the most commonly known vulnerabilities exploited by sophisticated foreign cyber actors.

This alert provides details on vulnerabilities routinely exploited by foreign cyber actors—primarily Common Vulnerabilities and Exposures (CVEs)[1]—to help organizations reduce the risk of these foreign threats.

Foreign cyber actors continue to exploit publicly known—and often dated—software vulnerabilities against broad target sets, including public and private sector organizations. Exploitation of these vulnerabilities often requires fewer resources as compared with zero-day exploits for which no patches are available.

The public and private sectors could degrade some foreign cyber threats to U.S. interests through an increased effort to patch their systems and implement programs to keep system patching up to date. A concerted campaign to patch these vulnerabilities would introduce friction into foreign adversaries' operational tradecraft and force them to develop or acquire exploits that are more costly and less widely effective. A concerted patching campaign would also bolster network security by focusing scarce defensive resources on the observed activities of foreign adversaries.

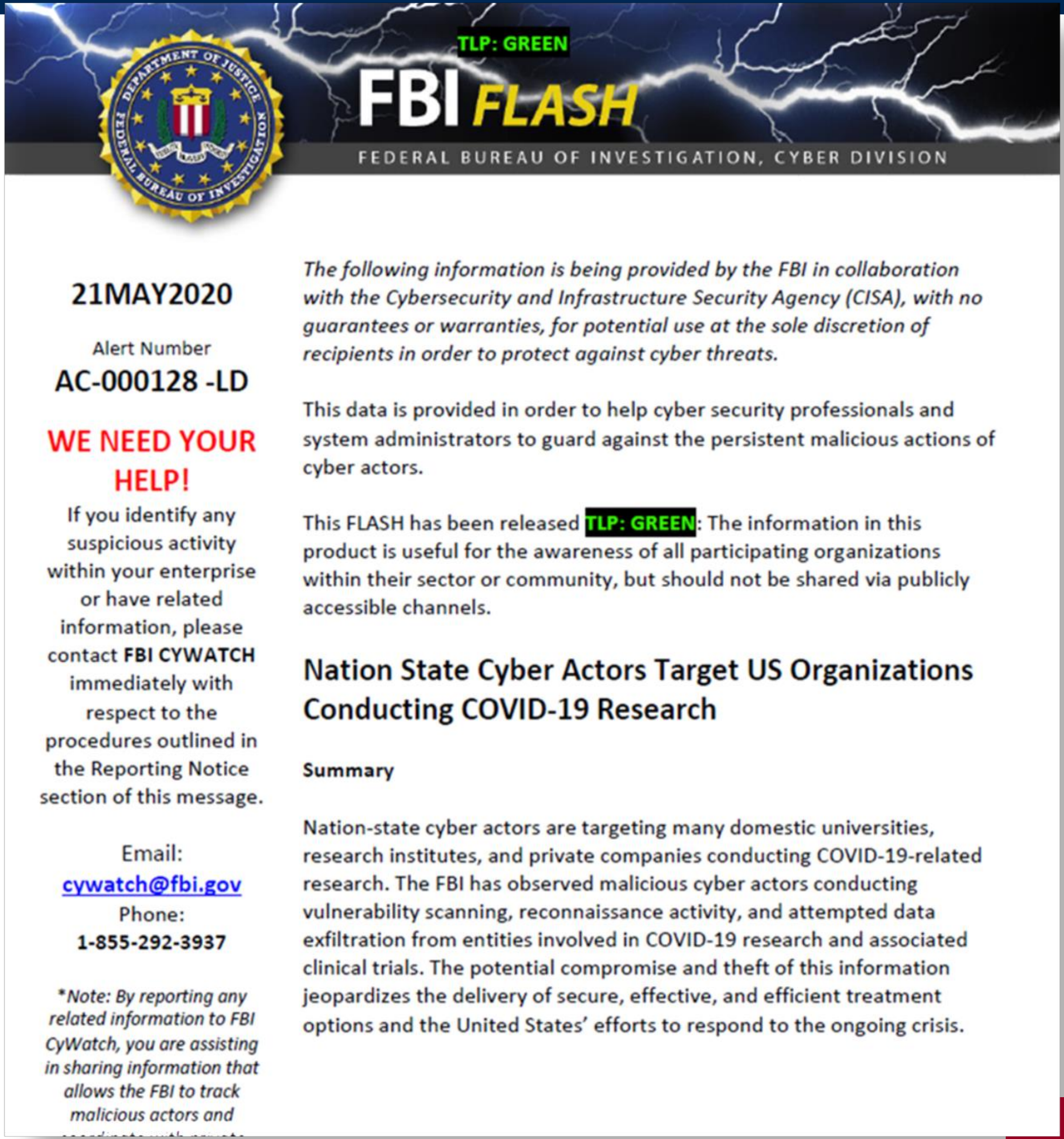
For Malware Initial Finding Reports and Malware Analysis reports associated with the CVEs in this alert, see https://www.us-cert.gov/ncas/alerts/aa20-133a.

https://www.us-cert.gov/ncas/alerts/aa20-133a

[1] https://cve.mitre.org/cve/

This document is marked TLP:WHITE. Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction. For more information on the Traffic Light Protocol, see http://www.us-cert.gov/tlp/.

TLP:WHITE



TLP: GREEN

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

21MAY2020

Alert Number

AC-000128 -LD

WE NEED YOUR HELP!

If you identify any suspicious activity within your enterprise or have related information, please contact **FBI CYWATCH** immediately with respect to the procedures outlined in the Reporting Notice section of this message.

Email:
cywatch@fbi.gov
Phone:
1-855-292-3937

**Note: By reporting any related information to FBI CyWatch, you are assisting in sharing information that allows the FBI to track malicious actors and*

The following information is being provided by the FBI in collaboration with the Cybersecurity and Infrastructure Security Agency (CISA), with no guarantees or warranties, for potential use at the sole discretion of recipients in order to protect against cyber threats.

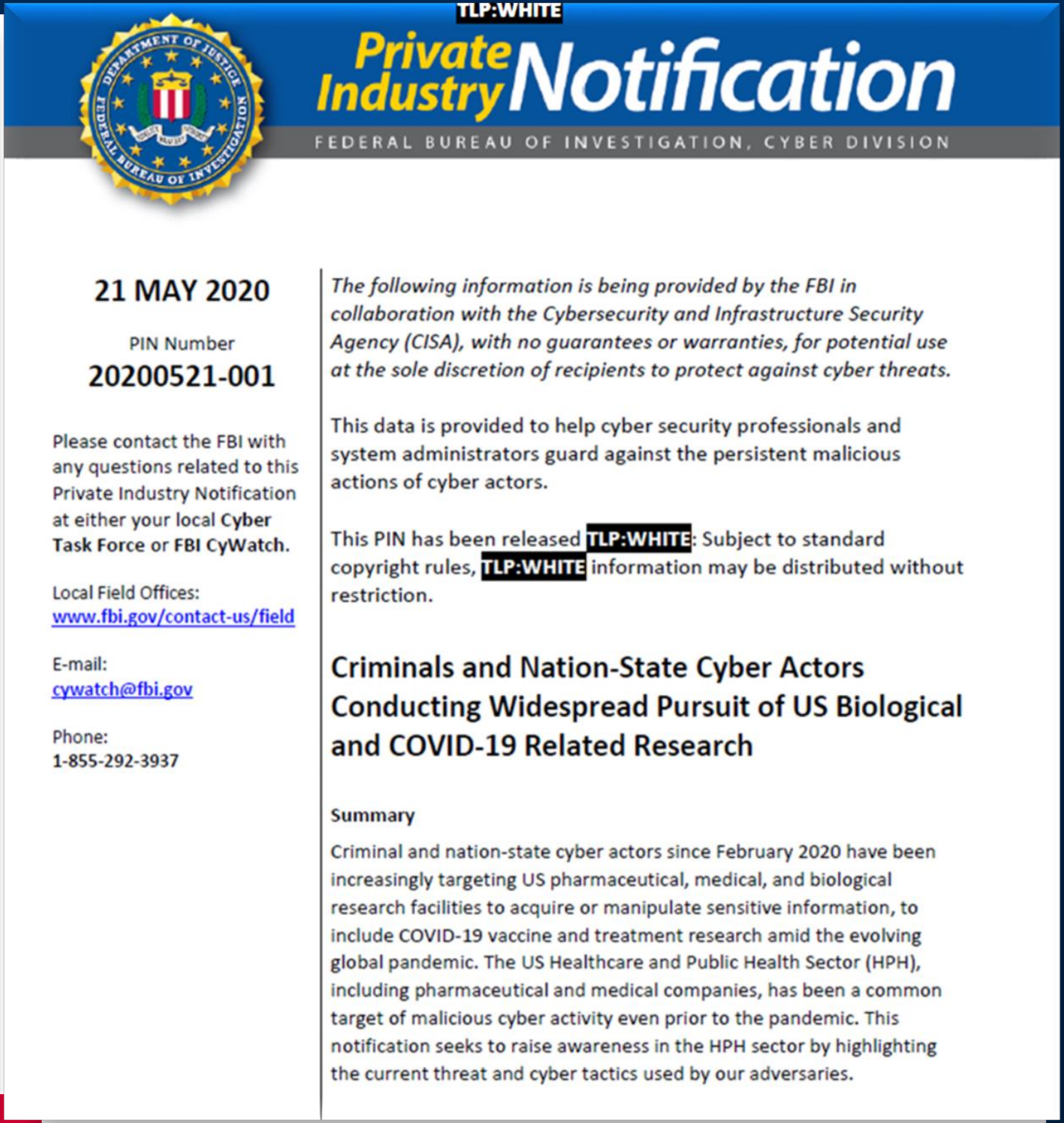
This data is provided in order to help cyber security professionals and system administrators to guard against the persistent malicious actions of cyber actors.

This FLASH has been released **TLP: GREEN**: The information in this product is useful for the awareness of all participating organizations within their sector or community, but should not be shared via publicly accessible channels.

Nation State Cyber Actors Target US Organizations Conducting COVID-19 Research

Summary

Nation-state cyber actors are targeting many domestic universities, research institutes, and private companies conducting COVID-19-related research. The FBI has observed malicious cyber actors conducting vulnerability scanning, reconnaissance activity, and attempted data exfiltration from entities involved in COVID-19 research and associated clinical trials. The potential compromise and theft of this information jeopardizes the delivery of secure, effective, and efficient treatment options and the United States' efforts to respond to the ongoing crisis.



TLP:WHITE

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

21 MAY 2020

PIN Number

20200521-001

Please contact the FBI with any questions related to this Private Industry Notification at either your local **Cyber Task Force** or **FBI CyWatch.**

Local Field Offices:
www.fbi.gov/contact-us/field

E-mail:
cywatch@fbi.gov

Phone:
1-855-292-3937

The following information is being provided by the FBI in collaboration with the Cybersecurity and Infrastructure Security Agency (CISA), with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats.

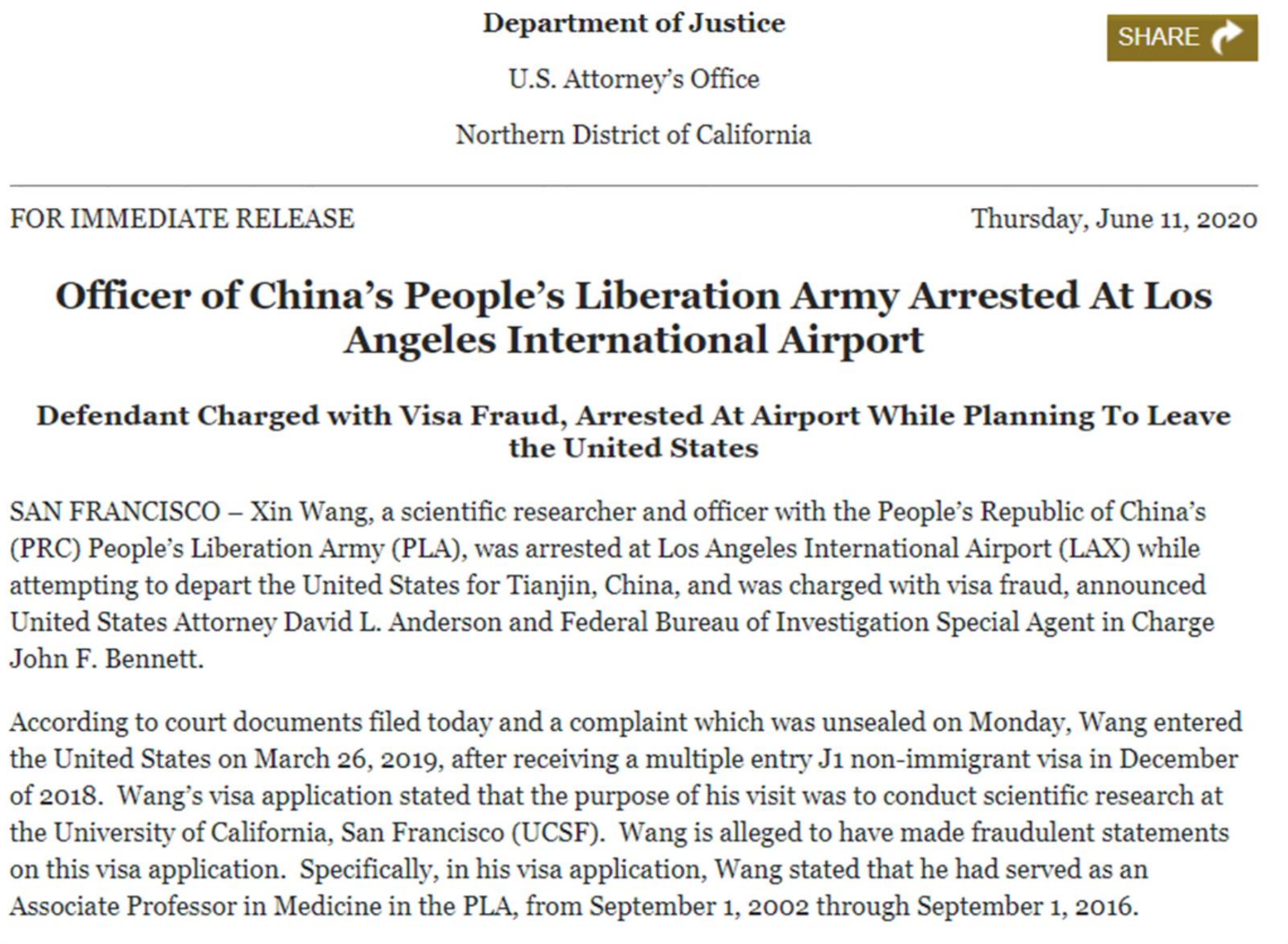
This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors.

This PIN has been released **TLP:WHITE**: Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction.

Criminals and Nation-State Cyber Actors Conducting Widespread Pursuit of US Biological and COVID-19 Related Research

Summary

Criminal and nation-state cyber actors since February 2020 have been increasingly targeting US pharmaceutical, medical, and biological research facilities to acquire or manipulate sensitive information, to include COVID-19 vaccine and treatment research amid the evolving global pandemic. The US Healthcare and Public Health Sector (HPH), including pharmaceutical and medical companies, has been a common target of malicious cyber activity even prior to the pandemic. This notification seeks to raise awareness in the HPH sector by highlighting the current threat and cyber tactics used by our adversaries.



Department of Justice

U.S. Attorney's Office

Northern District of California

SHARE

FOR IMMEDIATE RELEASE

Thursday, June 11, 2020

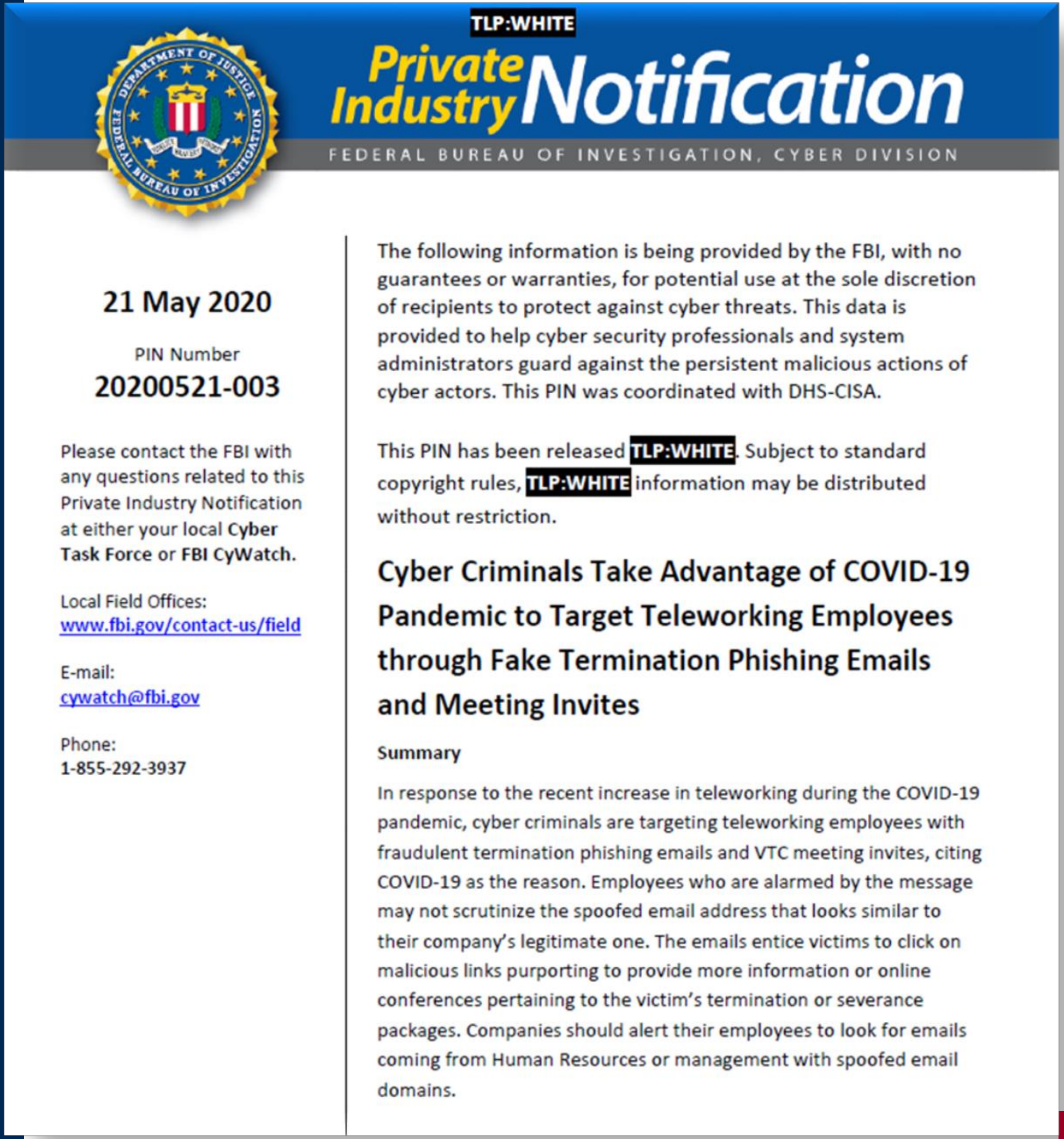
Officer of China's People's Liberation Army Arrested At Los Angeles International Airport

Defendant Charged with Visa Fraud, Arrested At Airport While Planning To Leave the United States

SAN FRANCISCO – Xin Wang, a scientific researcher and officer with the People's Republic of China's (PRC) People's Liberation Army (PLA), was arrested at Los Angeles International Airport (LAX) while attempting to depart the United States for Tianjin, China, and was charged with visa fraud, announced United States Attorney David L. Anderson and Federal Bureau of Investigation Special Agent in Charge John F. Bennett.

According to court documents filed today and a complaint which was unsealed on Monday, Wang entered the United States on March 26, 2019, after receiving a multiple entry J1 non-immigrant visa in December of 2018. Wang's visa application stated that the purpose of his visit was to conduct scientific research at the University of California, San Francisco (UCSF). Wang is alleged to have made fraudulent statements on this visa application. Specifically, in his visa application, Wang stated that he had served as an Associate Professor in Medicine in the PLA, from September 1, 2002 through September 1, 2016.

© REUTERS



TLP:WHITE

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

21 May 2020

PIN Number

20200521-003

Please contact the FBI with any questions related to this Private Industry Notification at either your local **Cyber Task Force** or **FBI CyWatch.**

Local Field Offices:
www.fbi.gov/contact-us/field

E-mail:
cywatch@fbi.gov

Phone:
1-855-292-3937

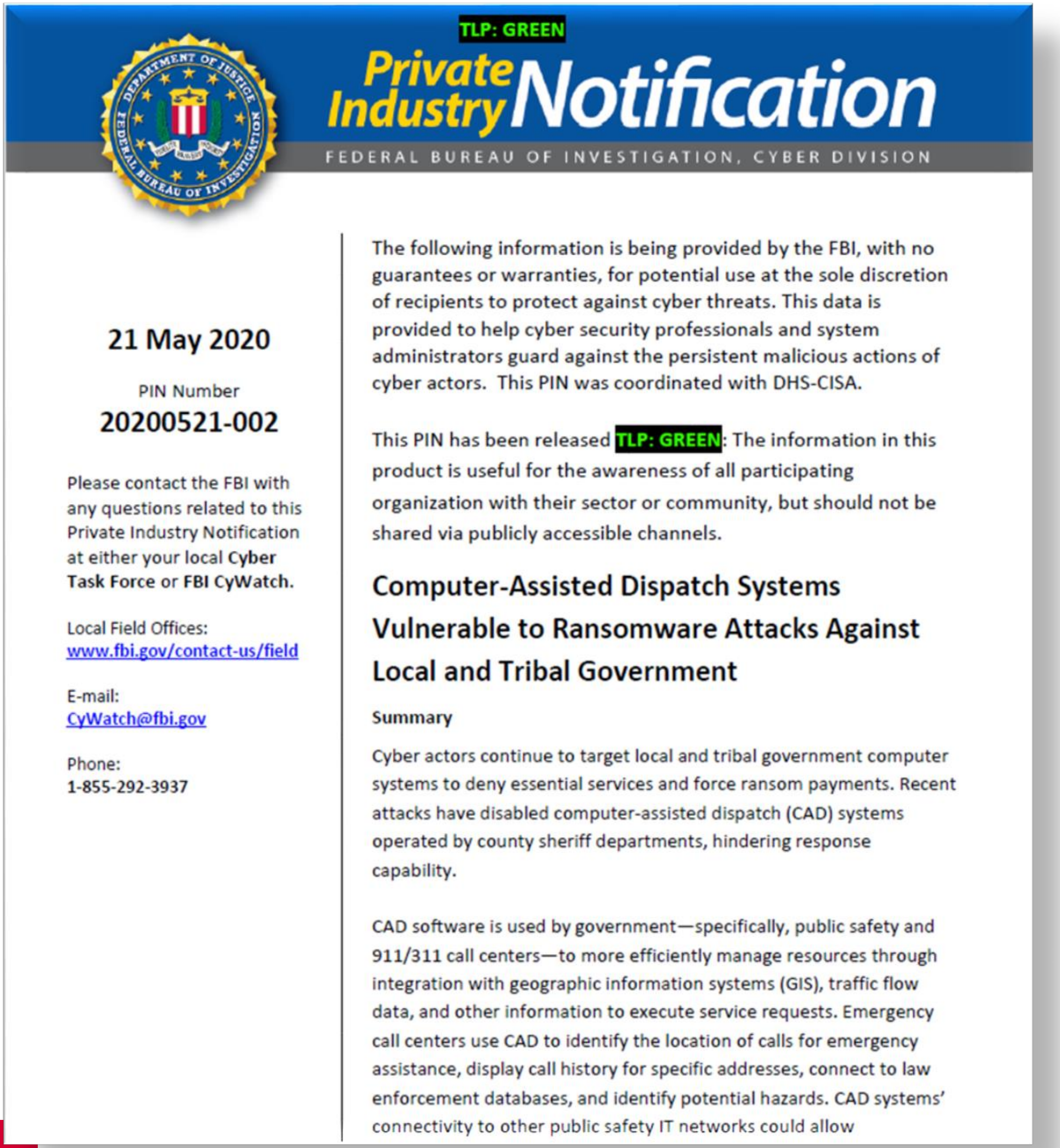
The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors. This PIN was coordinated with DHS-CISA.

This PIN has been released **TLP:WHITE**. Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction.

Cyber Criminals Take Advantage of COVID-19 Pandemic to Target Teleworking Employees through Fake Termination Phishing Emails and Meeting Invites

Summary

In response to the recent increase in teleworking during the COVID-19 pandemic, cyber criminals are targeting teleworking employees with fraudulent termination phishing emails and VTC meeting invites, citing COVID-19 as the reason. Employees who are alarmed by the message may not scrutinize the spoofed email address that looks similar to their company's legitimate one. The emails entice victims to click on malicious links purporting to provide more information or online conferences pertaining to the victim's termination or severance packages. Companies should alert their employees to look for emails coming from Human Resources or management with spoofed email domains.



TLP: GREEN

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

21 May 2020

PIN Number

20200521-002

Please contact the FBI with any questions related to this Private Industry Notification at either your local **Cyber Task Force** or **FBI CyWatch.**

Local Field Offices:
www.fbi.gov/contact-us/field

E-mail:
CyWatch@fbi.gov

Phone:
1-855-292-3937

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors. This PIN was coordinated with DHS-CISA.

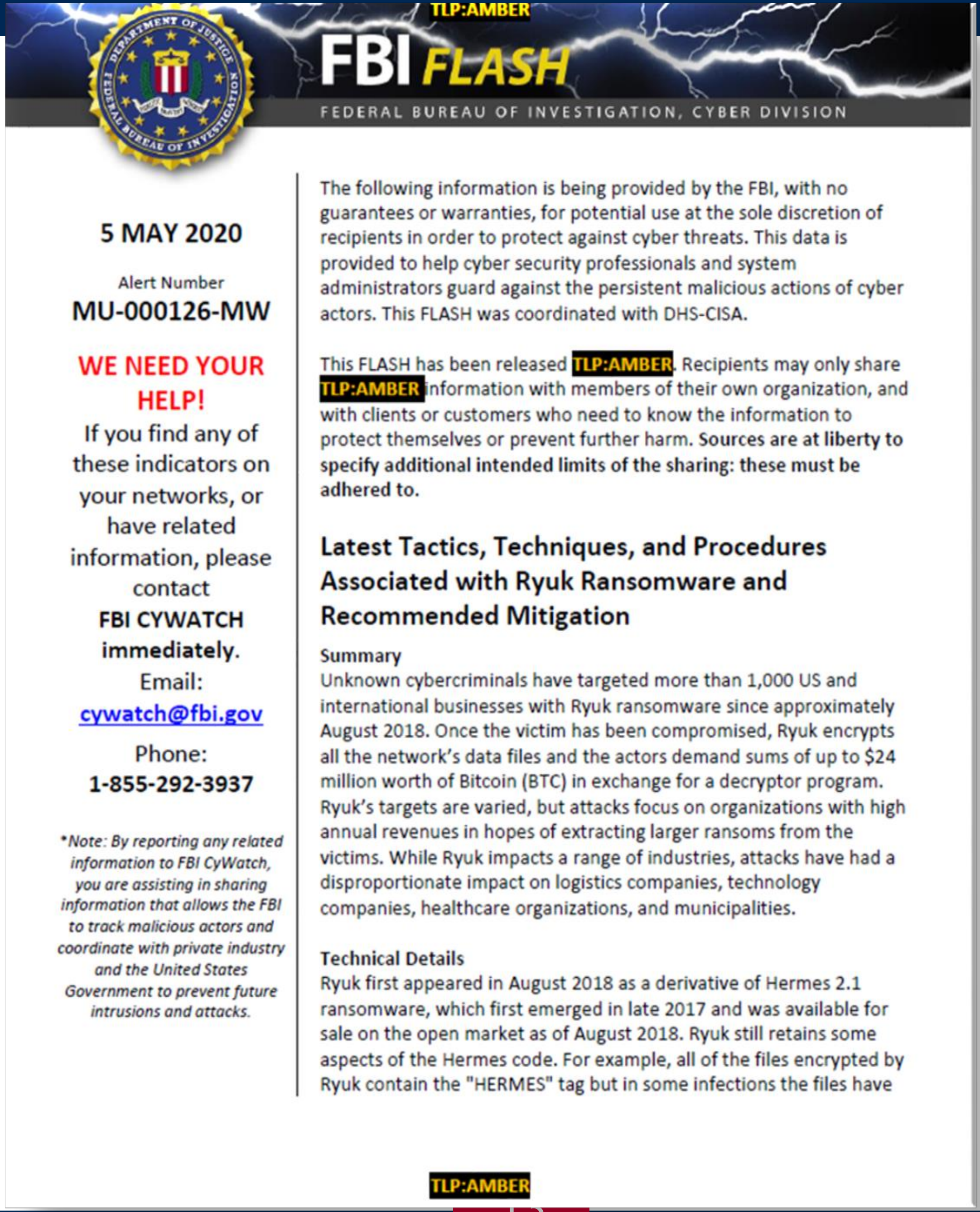
This PIN has been released **TLP: GREEN**: The information in this product is useful for the awareness of all participating organization with their sector or community, but should not be shared via publicly accessible channels.

Computer-Assisted Dispatch Systems Vulnerable to Ransomware Attacks Against Local and Tribal Government

Summary

Cyber actors continue to target local and tribal government computer systems to deny essential services and force ransom payments. Recent attacks have disabled computer-assisted dispatch (CAD) systems operated by county sheriff departments, hindering response capability.

CAD software is used by government—specifically, public safety and 911/311 call centers—to more efficiently manage resources through integration with geographic information systems (GIS), traffic flow data, and other information to execute service requests. Emergency call centers use CAD to identify the location of calls for emergency assistance, display call history for specific addresses, connect to law enforcement databases, and identify potential hazards. CAD systems' connectivity to other public safety IT networks could allow



TLP:AMBER

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

5 MAY 2020

Alert Number

MU-000126-MW

WE NEED YOUR HELP!

If you find any of these indicators on your networks, or have related information, please contact

FBI CYWATCH immediately.

Email:

cywatch@fbi.gov

Phone:

1-855-292-3937

**Note: By reporting any related information to FBI CyWatch, you are assisting in sharing information that allows the FBI to track malicious actors and coordinate with private industry and the United States Government to prevent future intrusions and attacks.*

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients in order to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors. This FLASH was coordinated with DHS-CISA.

This FLASH has been released **TLP:AMBER**. Recipients may only share **TLP:AMBER** information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**

Latest Tactics, Techniques, and Procedures Associated with Ryuk Ransomware and Recommended Mitigation

Summary

Unknown cybercriminals have targeted more than 1,000 US and international businesses with Ryuk ransomware since approximately August 2018. Once the victim has been compromised, Ryuk encrypts all the network's data files and the actors demand sums of up to $24 million worth of Bitcoin (BTC) in exchange for a decryptor program. Ryuk's targets are varied, but attacks focus on organizations with high annual revenues in hopes of extracting larger ransoms from the victims. While Ryuk impacts a range of industries, attacks have had a disproportionate impact on logistics companies, technology companies, healthcare organizations, and municipalities.

Technical Details

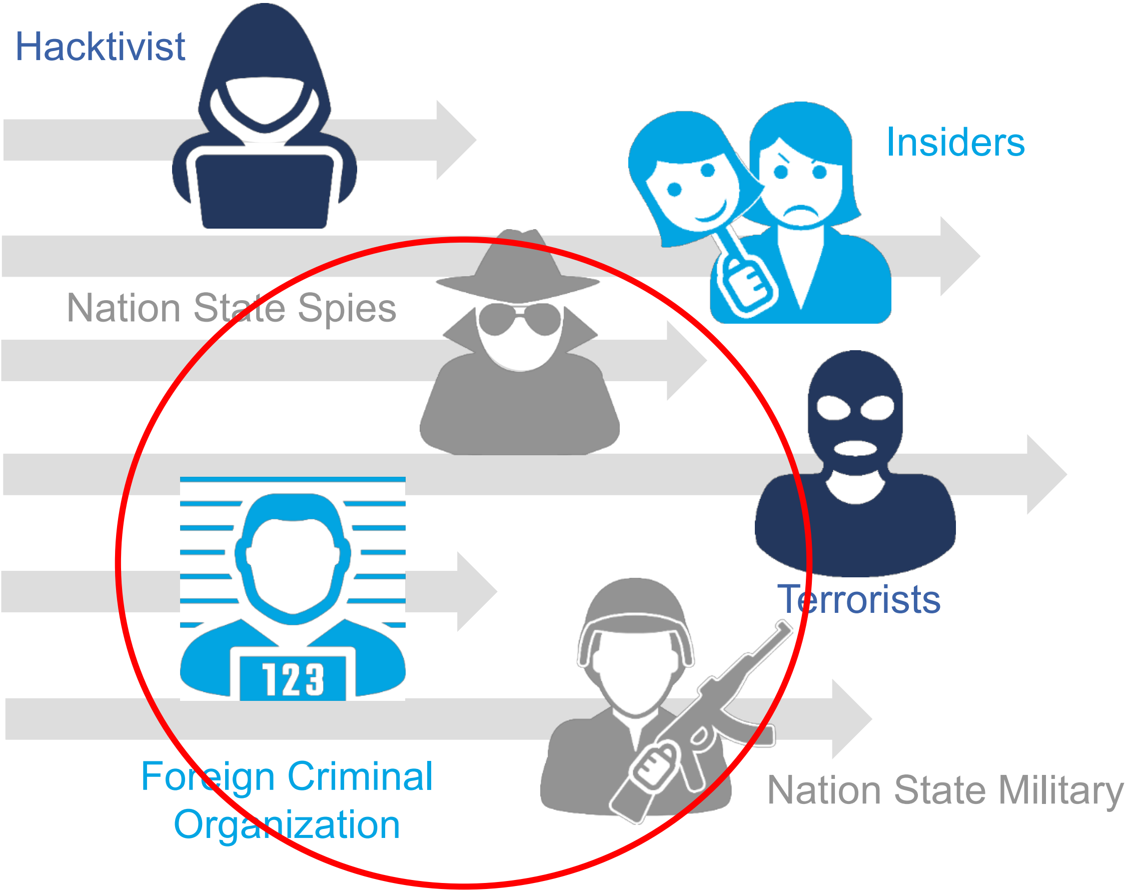
Ryuk first appeared in August 2018 as a derivative of Hermes 2.1 ransomware, which first emerged in late 2017 and was available for sale on the open market as of August 2018. Ryuk still retains some aspects of the Hermes code. For example, all of the files encrypted by Ryuk contain the "HERMES" tag but in some infections the files have

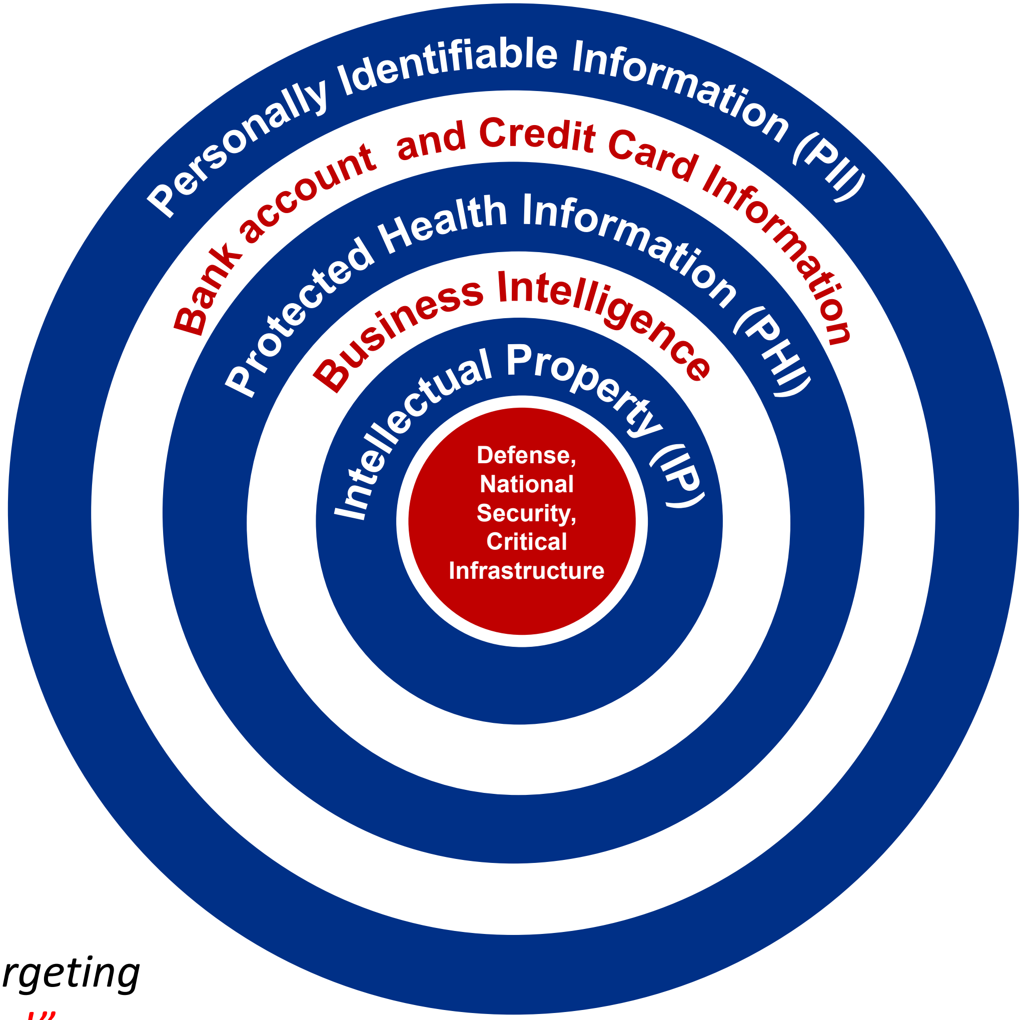
TLP:AMBER

Comments and Questions?

Data Rich Environment = Target Rich Environment

Targeted Data

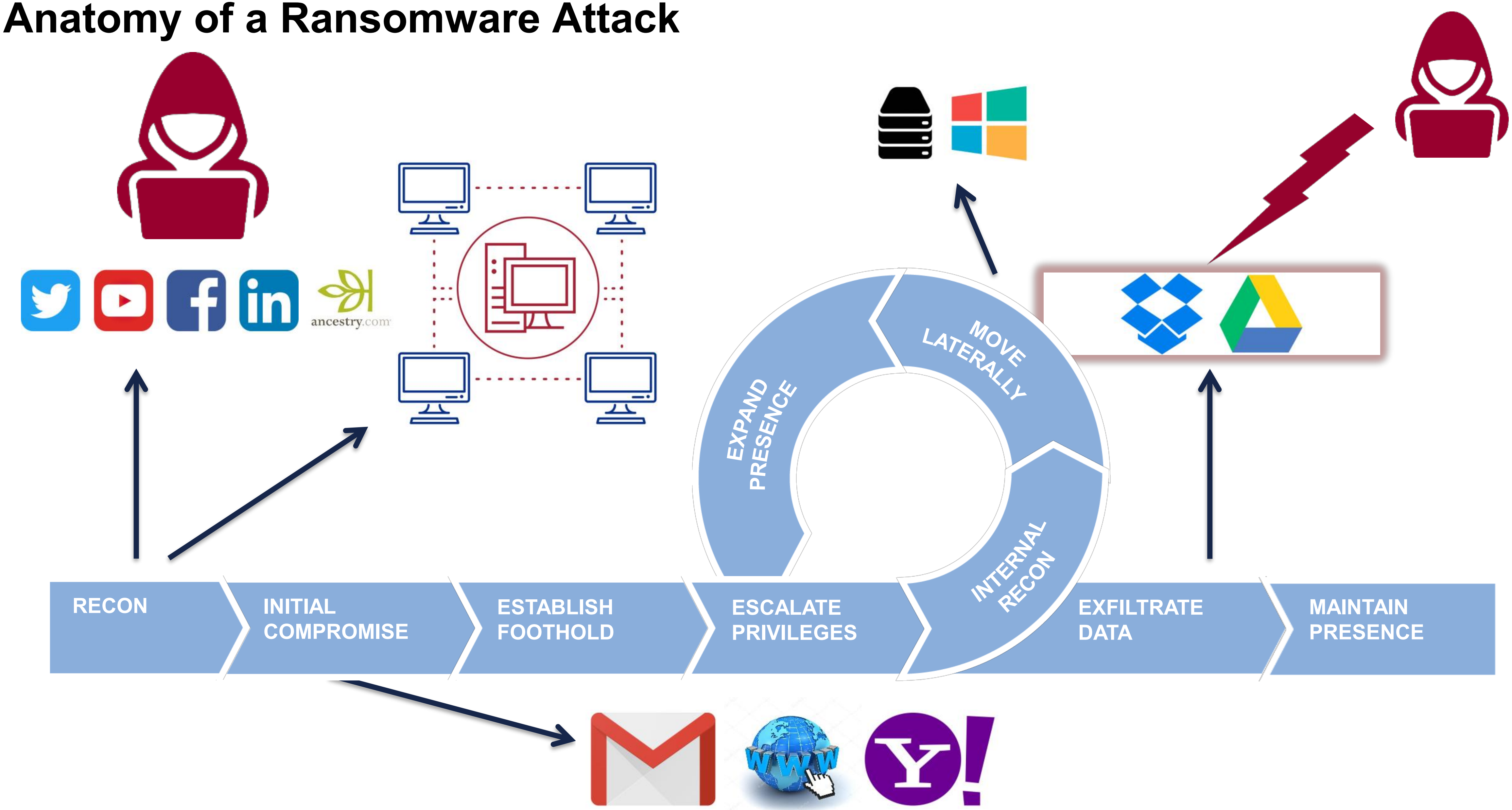




Personally Identifiable Information (PII)
Bank account and Credit Card Information
Protected Health Information (PHI)
Business Intelligence
Intellectual Property (IP)
Defense, National Security, Critical Infrastructure

Nation states, criminals, insiders and hacktivists are aggressively targeting healthcare providers to steal their valuable data. ***"One stop hacking!"***

Anatomy of a Ransomware Attack



RECON

INITIAL COMPROMISE

ESTABLISH FOOTHOLD

ESCALATE PRIVILEGES

EXPAND PRESENCE

MOVE LATERALLY

INTERNAL RECON

EXFILTRATE DATA

MAINTAIN PRESENCE

Types of Social Media

- There are many categories of social media, the most common:
  Social Networking
  - Examples:
    - Facebook
    - Myspace (obsolete)
    - Google (obsolete)
    - LinkedIn
    - Twitter
- Many other categories:
  - Pictures/Images
    - Snap Chat
    - Instagram
    - Flickr
  - Knowledge/Discussion
    - Wikipedia
    - Academia
    - Reddit
  - Music
    - Pandora
    - Spotify
    - Rhapsody

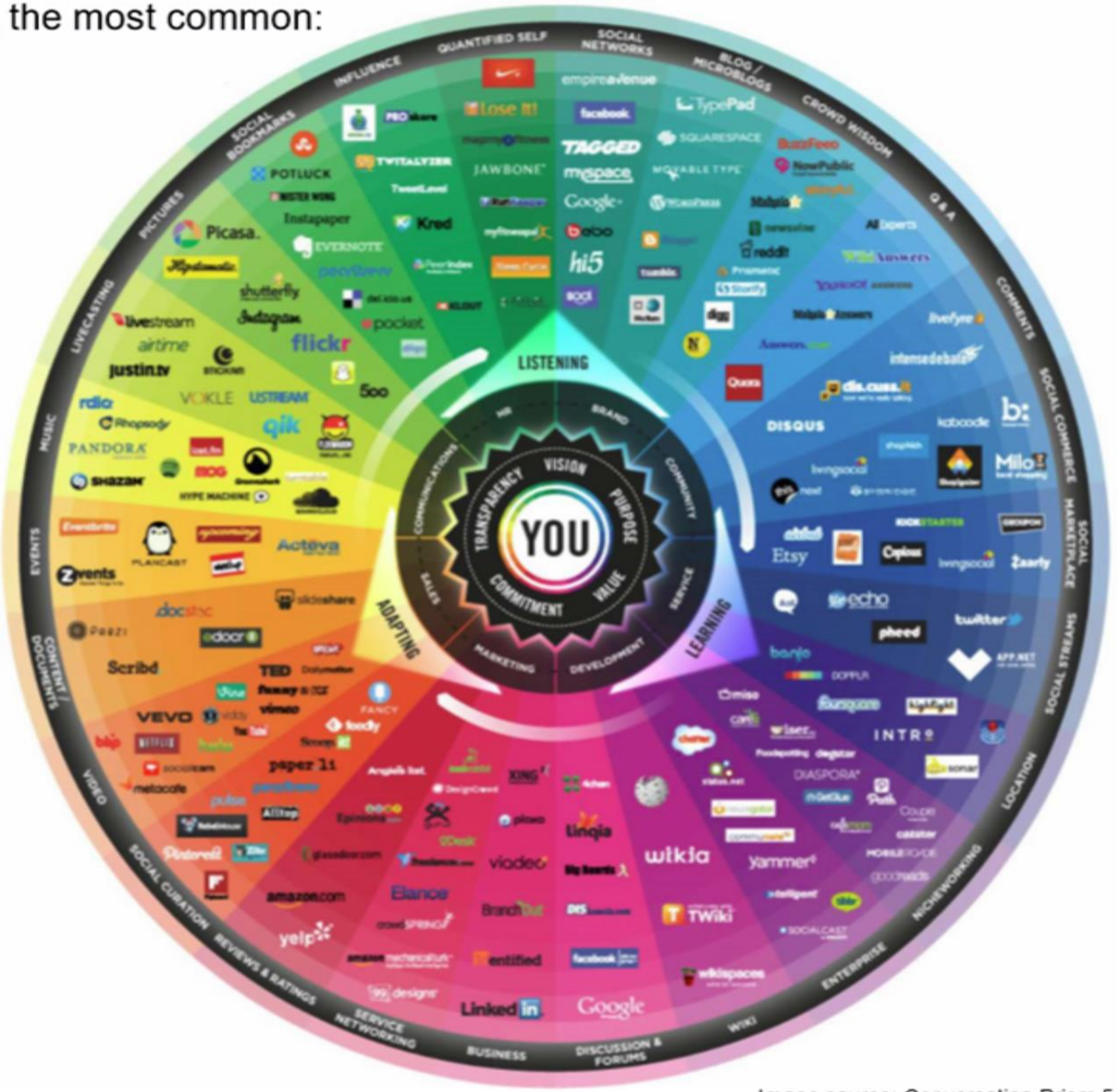


Image source: Conversation Prism 5.0

Impact of Social Media Breaches

- While breaches of social media websites/companies only make up less than one percent of all data breaches per year, the incidents account for over 56% of ALL compromised data.

Google+

Affected Users
2018: 52.5 Million

Twitter

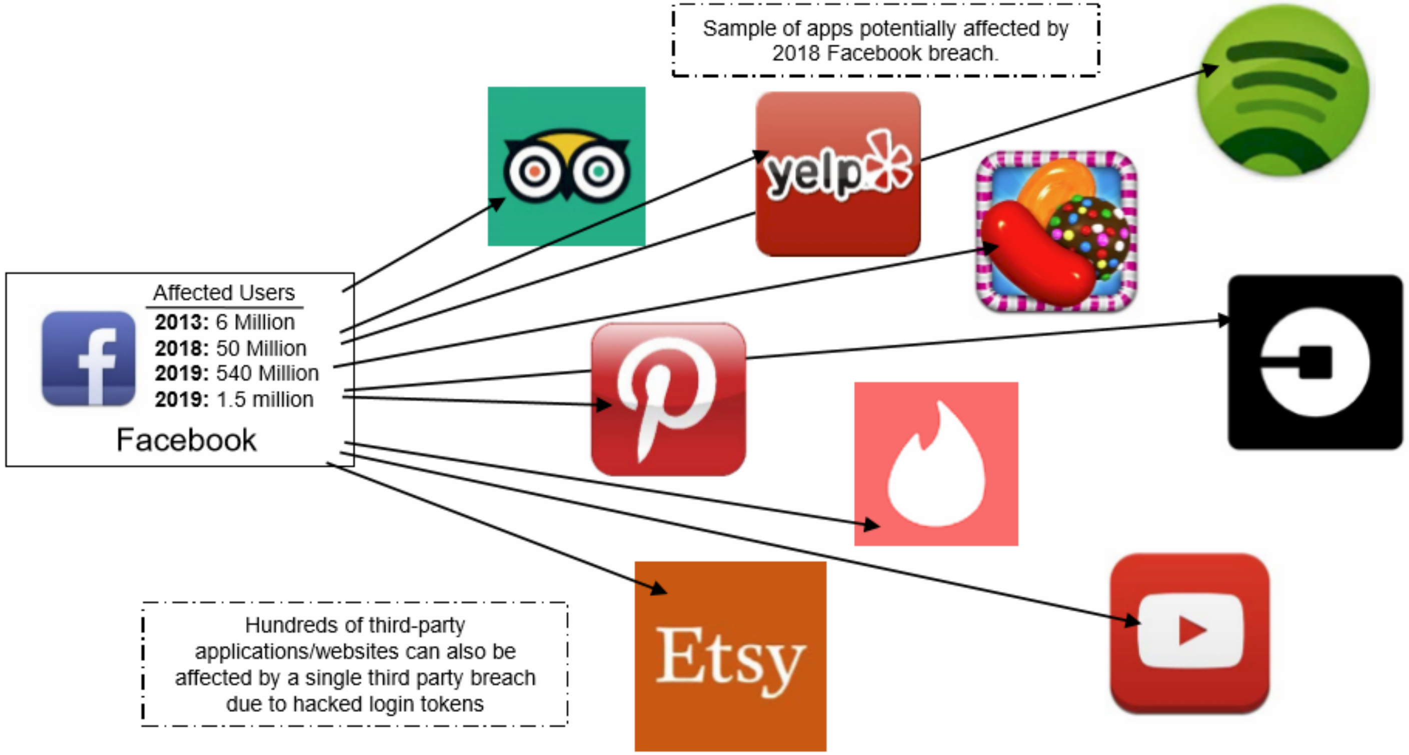
Affected Users
2013: 250,000
2016: 32.8 Million
2018: 330 Million

Snapchat

Affected Users
2013: 4.6 Million
2017: 55,000

LinkedIn

Affected Users
2012: 6.5 Million
2016: 167 Million



Facebook

Affected Users
2013: 6 Million
2018: 50 Million
2019: 540 Million
2019: 1.5 million

Sample of apps potentially affected by 2018 Facebook breach.

Hundreds of third-party applications/websites can also be affected by a single third party breach due to hacked login tokens

The extent to how much specific data is compromised across the internet due to a single social media breach still can not be ascertained due to the sheer amount of apps than can be accessed with third party login credentials.

Comments and Questions?

PRIVATE

Detection and Risk Controls: *EG - 3C*

- **EDUCATE -** Create awareness and support among leadership, researchers and staff *in an audience sensitive manner,* of the foreign influence threats to medical research and innovation. Discuss real world implications.
- **GOVERNANCE -** Identify a function and senior accountable executive who will have overall responsibility and sufficient independence, authority and status to coordinate and lead the process across multiple functions.

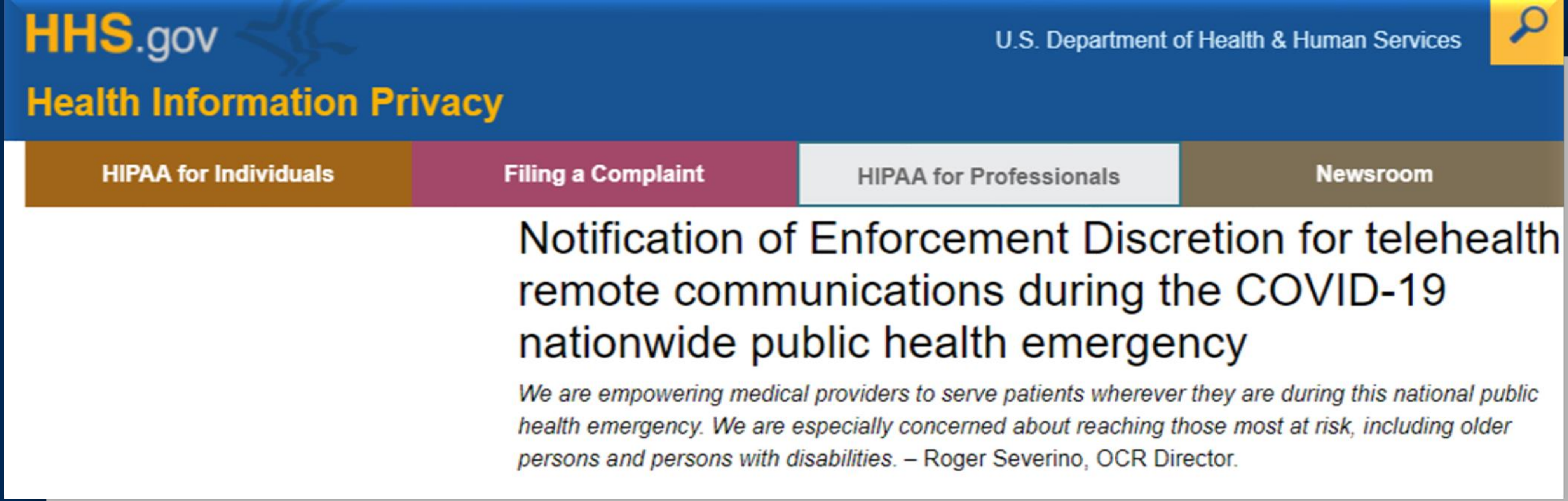
- **CATALOGUE** - All research and intellectual property
  - Where are the ***multiple*** locations it is stored, ***who has access, internally and remotely*** ?
- Risk **CLASSIFY and STRATIFY** research data in terms of impact to:
  - Public Health and Safety
  - Dual Use – Military Application, weaponization
  - National Security
  - Economic Security
  - Business Risk – What is the value? Strategic implications, economic value, loss of innovation, reputation.
- Outside expertise and government assistance (FBI, DHS, HHS, NIH and Commerce) - ***Ongoing Process***
- **CONTROL** – Based upon risk classification and stratification. Combination of personnel, legal, physical and information security controls.

Risk Prioritization and Impact

Do we prioritize all strategic threats, cybersecurity policies, procedures, controls and technical risks by ***impact*** to:

REPUTATION

1. ***Care delivery and PATIENT SAFETY - first and always***
2. Mission critical operations
3. Confidence of patients, staff, community and investors
4. Protection and privacy of data - including health records, personally identifiable information, financial and payment data and intellectual property*
5. Revenue
6. Legal and regulatory exposure
7. Mergers and acquisitions



Notification of Enforcement Discretion for telehealth remote communications during the COVID-19 nationwide public health emergency

We are empowering medical providers to serve patients wherever they are during this national public health emergency. We are especially concerned about reaching those most at risk, including older persons and persons with disabilities. – Roger Severino, OCR Director.

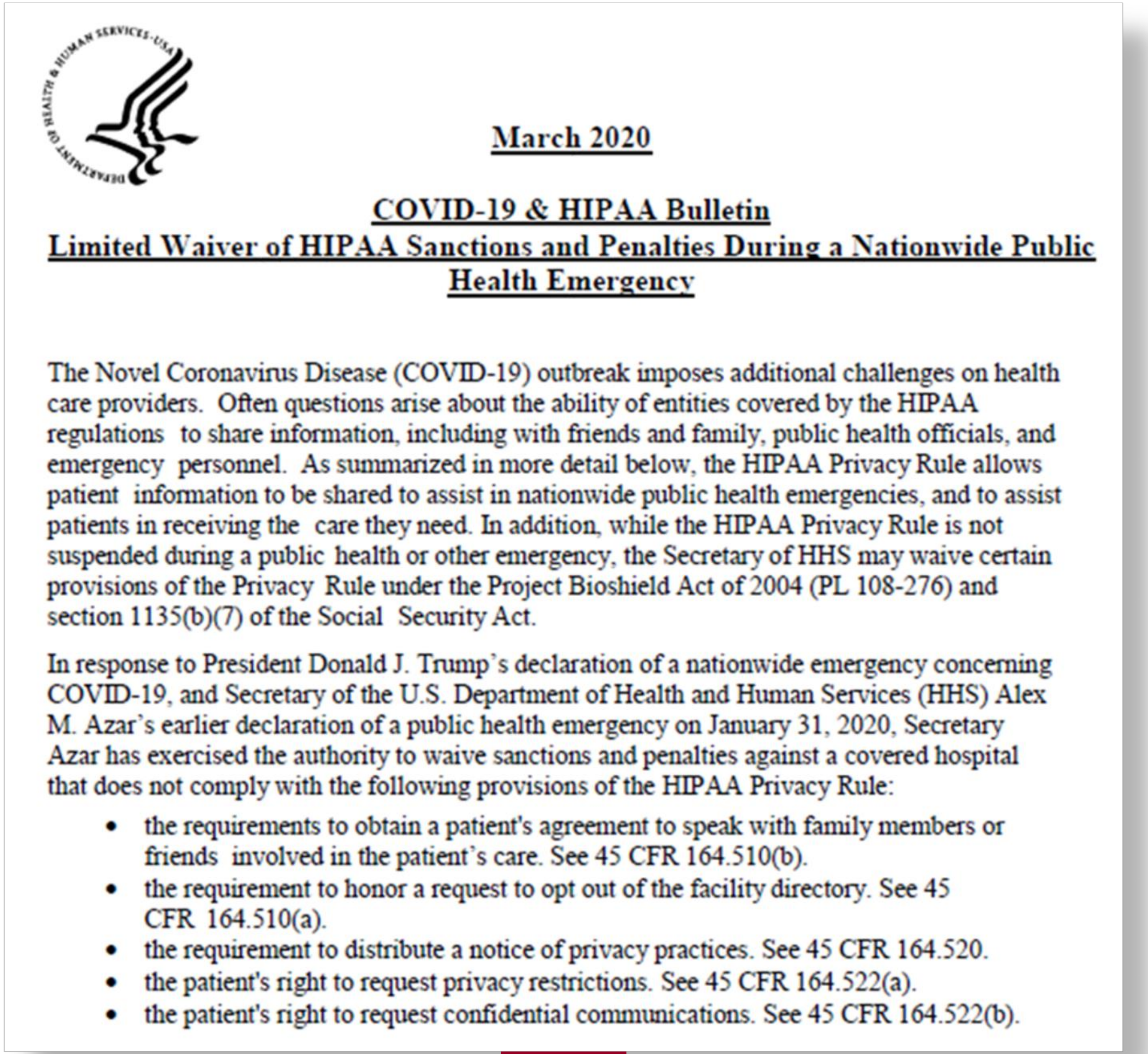
Telehealth vulnerabilities
American Hospital Association
Advancing Health in America

Non-public facing technologies, such as FaceTime or Skype allowed.

Good faith provision of telehealth during the COVID-19 nationwide public health emergency

Public facing apps such as Facebook Live, Twitch, TikTok, and similar are prohibited

Notify patients that these third-party applications potentially introduce privacy risks, and providers should enable all available encryption and privacy modes



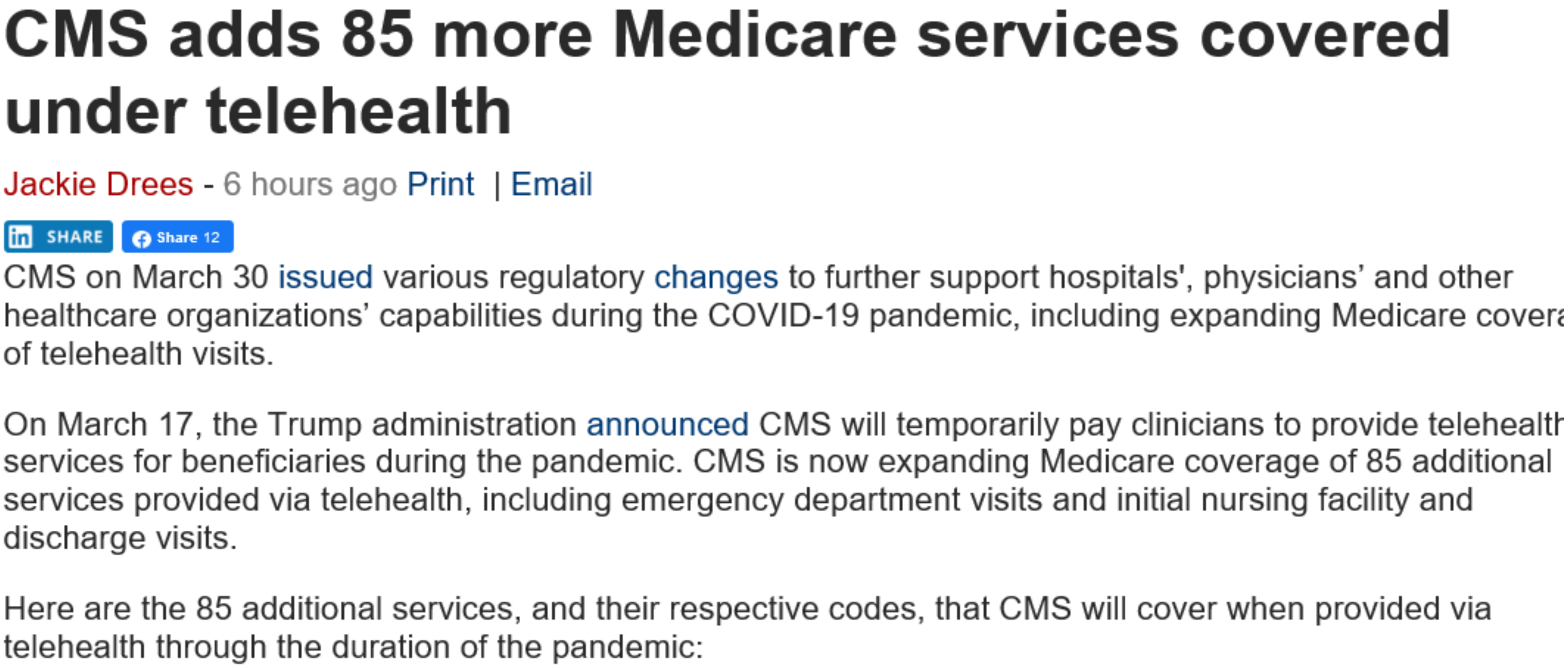
March 2020

COVID-19 & HIPAA Bulletin
Limited Waiver of HIPAA Sanctions and Penalties During a Nationwide Public Health Emergency

The Novel Coronavirus Disease (COVID-19) outbreak imposes additional challenges on health care providers. Often questions arise about the ability of entities covered by the HIPAA regulations to share information, including with friends and family, public health officials, and emergency personnel. As summarized in more detail below, the HIPAA Privacy Rule allows patient information to be shared to assist in nationwide public health emergencies, and to assist patients in receiving the care they need. In addition, while the HIPAA Privacy Rule is not suspended during a public health or other emergency, the Secretary of HHS may waive certain provisions of the Privacy Rule under the Project Bioshield Act of 2004 (PL 108-276) and section 1135(b)(7) of the Social Security Act.

In response to President Donald J. Trump's declaration of a nationwide emergency concerning COVID-19, and Secretary of the U.S. Department of Health and Human Services (HHS) Alex M. Azar's earlier declaration of a public health emergency on January 31, 2020, Secretary Azar has exercised the authority to waive sanctions and penalties against a covered hospital that does not comply with the following provisions of the HIPAA Privacy Rule:

- the requirements to obtain a patient's agreement to speak with family members or friends involved in the patient's care. See 45 CFR 164.510(b).
- the requirement to honor a request to opt out of the facility directory. See 45 CFR 164.510(a).
- the requirement to distribute a notice of privacy practices. See 45 CFR 164.520.
- the patient's right to request privacy restrictions. See 45 CFR 164.522(a).
- the patient's right to request confidential communications. See 45 CFR 164.522(b).



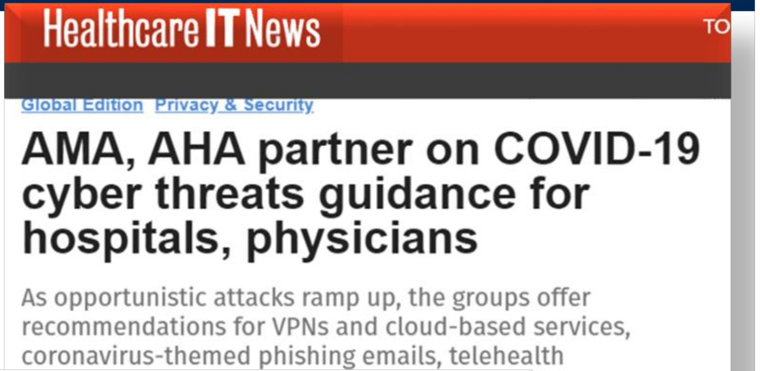
CMS adds 85 more Medicare services covered under telehealth

Jackie Drees - 6 hours ago Print | Email

CMS on March 30 issued various regulatory changes to further support hospitals', physicians' and other healthcare organizations' capabilities during the COVID-19 pandemic, including expanding Medicare covera of telehealth visits.

On March 17, the Trump administration announced CMS will temporarily pay clinicians to provide telehealth services for beneficiaries during the pandemic. CMS is now expanding Medicare coverage of 85 additional services provided via telehealth, including emergency department visits and initial nursing facility and discharge visits.

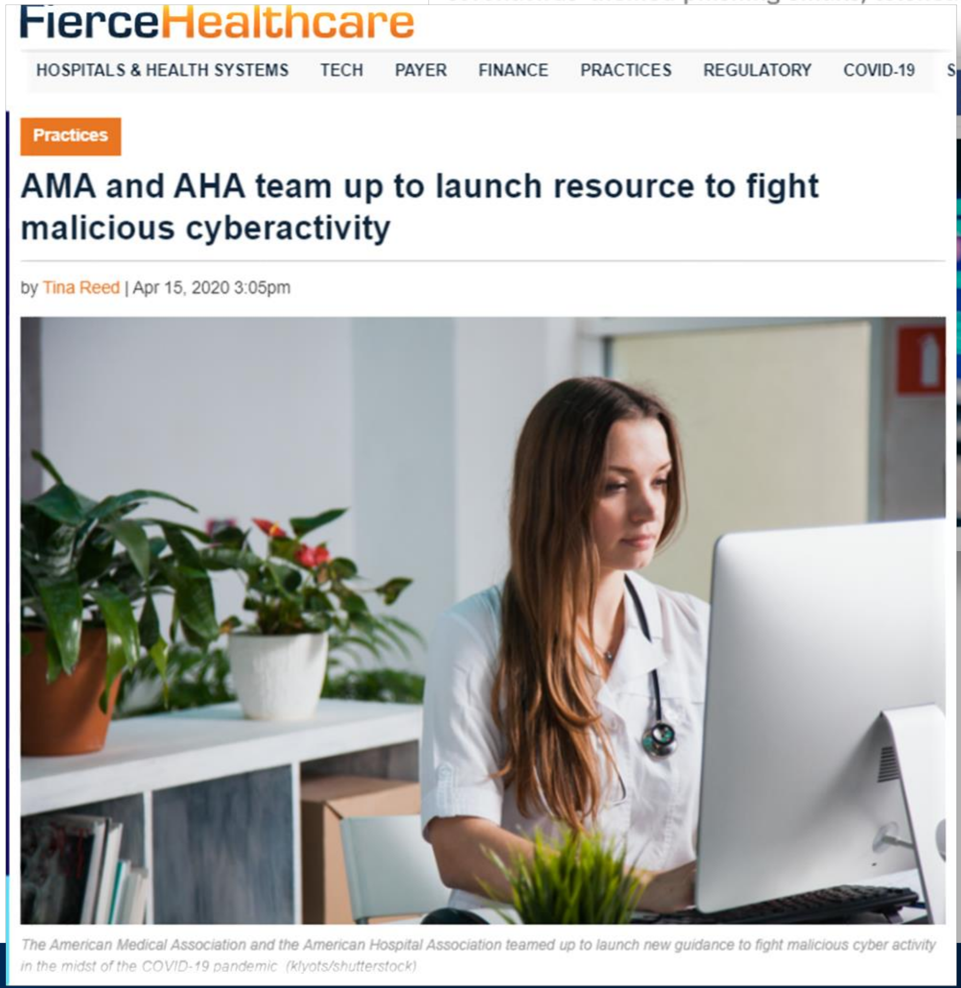
Here are the 85 additional services, and their respective codes, that CMS will cover when provided via telehealth through the duration of the pandemic:



Global Edition Privacy & Security

AMA, AHA partner on COVID-19 cyber threats guidance for hospitals, physicians

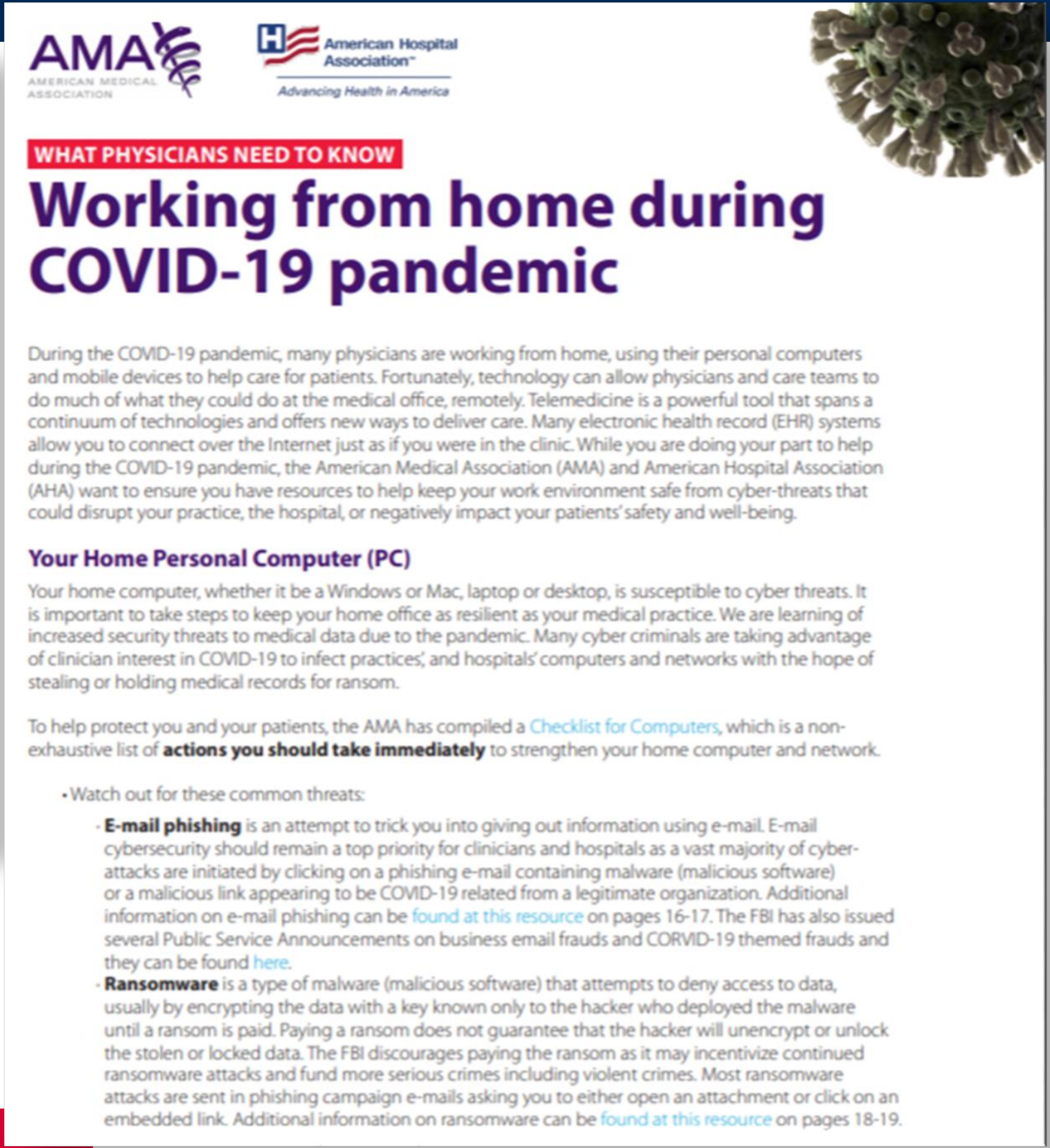
As opportunistic attacks ramp up, the groups offer recommendations for VPNs and cloud-based services, coronavirus-themed phishing emails, telehealth



AMA and AHA team up to launch resource to fight malicious cyberactivity

by Tina Reed | Apr 15, 2020 3:05pm

The American Medical Association and the American Hospital Association teamed up to launch new guidance to fight malicious cyber activity in the midst of the COVID-19 pandemic (klyots/shutterstock)



AMA
AMERICAN MEDICAL ASSOCIATION
American Hospital Association
Advancing Health in America

WHAT PHYSICIANS NEED TO KNOW

Working from home during COVID-19 pandemic

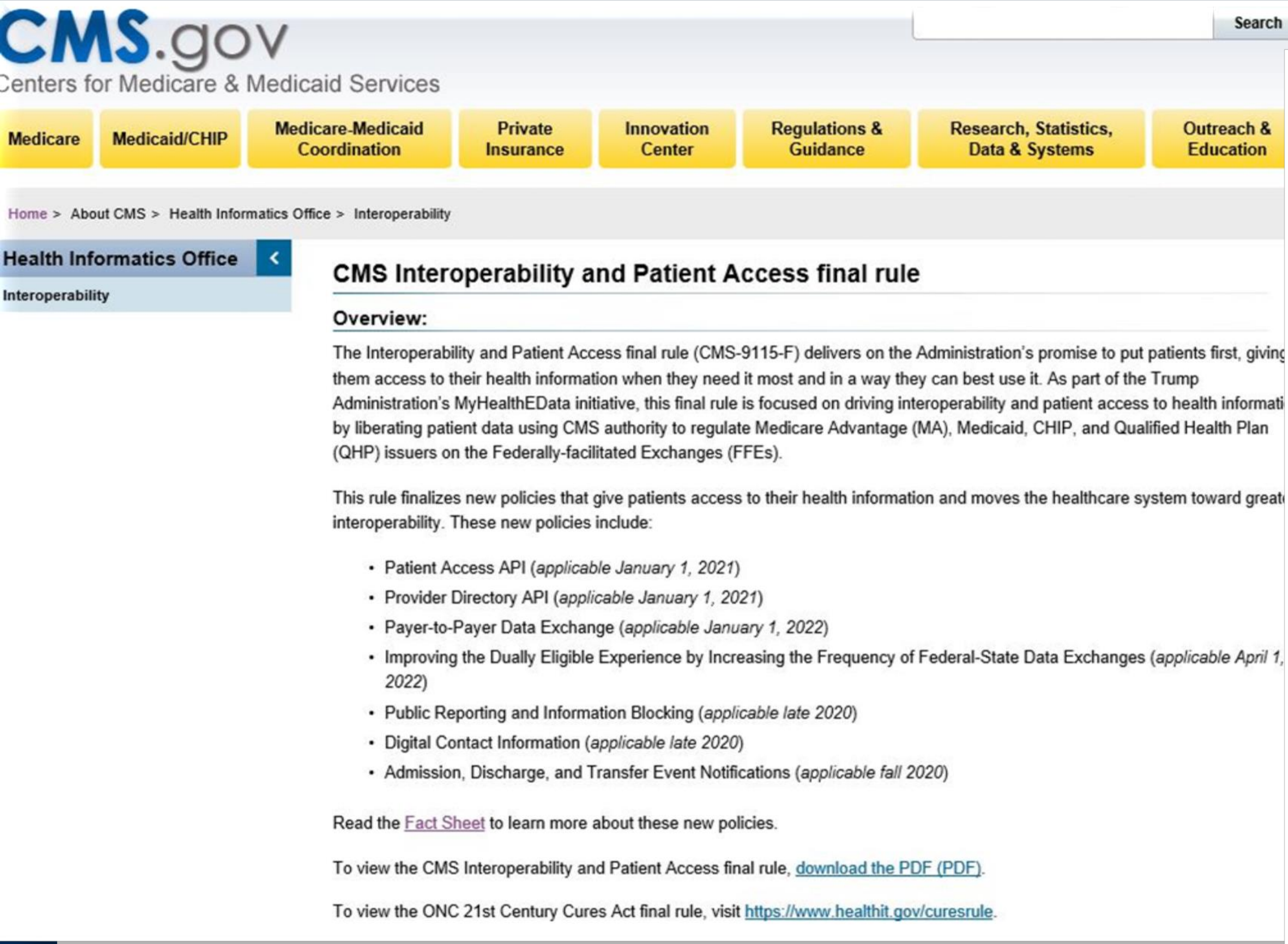
During the COVID-19 pandemic, many physicians are working from home, using their personal computers and mobile devices to help care for patients. Fortunately, technology can allow physicians and care teams to do much of what they could do at the medical office, remotely. Telemedicine is a powerful tool that spans a continuum of technologies and offers new ways to deliver care. Many electronic health record (EHR) systems allow you to connect over the Internet just as if you were in the clinic. While you are doing your part to help during the COVID-19 pandemic, the American Medical Association (AMA) and American Hospital Association (AHA) want to ensure you have resources to help keep your work environment safe from cyber-threats that could disrupt your practice, the hospital, or negatively impact your patients' safety and well-being.

Your Home Personal Computer (PC)

Your home computer, whether it be a Windows or Mac, laptop or desktop, is susceptible to cyber threats. It is important to take steps to keep your home office as resilient as your medical practice. We are learning of increased security threats to medical data due to the pandemic. Many cyber criminals are taking advantage of clinician interest in COVID-19 to infect practices' and hospitals' computers and networks with the hope of stealing or holding medical records for ransom.

To help protect you and your patients, the AMA has compiled a Checklist for Computers, which is a non-exhaustive list of **actions you should take immediately** to strengthen your home computer and network.

- Watch out for these common threats:
  - **E-mail phishing** is an attempt to trick you into giving out information using e-mail. E-mail cybersecurity should remain a top priority for clinicians and hospitals as a vast majority of cyber-attacks are initiated by clicking on a phishing e-mail containing malware (malicious software) or a malicious link appearing to be COVID-19 related from a legitimate organization. Additional information on e-mail phishing can be found at this resource on pages 16-17. The FBI has also issued several Public Service Announcements on business email frauds and CORVID-19 themed frauds and they can be found here.
  - **Ransomware** is a type of malware (malicious software) that attempts to deny access to data, usually by encrypting the data with a key known only to the hacker who deployed the malware until a ransom is paid. Paying a ransom does not guarantee that the hacker will unencrypt or unlock the stolen or locked data. The FBI discourages paying the ransom as it may incentivize continued ransomware attacks and fund more serious crimes including violent crimes. Most ransomware attacks are sent in phishing campaign e-mails asking you to either open an attachment or click on an embedded link. Additional information on ransomware can be found at this resource on pages 18-19.


CMS.gov
Centers for Medicare & Medicaid Services
Search
Medicare
Medicaid/CHIP
Medicare-Medicaid Coordination
Private Insurance
Innovation Center
Regulations & Guidance
Research, Statistics, Data & Systems
Outreach & Education
Home > About CMS > Health Informatics Office > Interoperability
Health Informatics Office
Interoperability

CMS Interoperability and Patient Access final rule

Overview:

The Interoperability and Patient Access final rule (CMS-9115-F) delivers on the Administration's promise to put patients first, giving them access to their health information when they need it most and in a way they can best use it. As part of the Trump Administration's MyHealthEData initiative, this final rule is focused on driving interoperability and patient access to health informati by liberating patient data using CMS authority to regulate Medicare Advantage (MA), Medicaid, CHIP, and Qualified Health Plan (QHP) issuers on the Federally-facilitated Exchanges (FFEs).

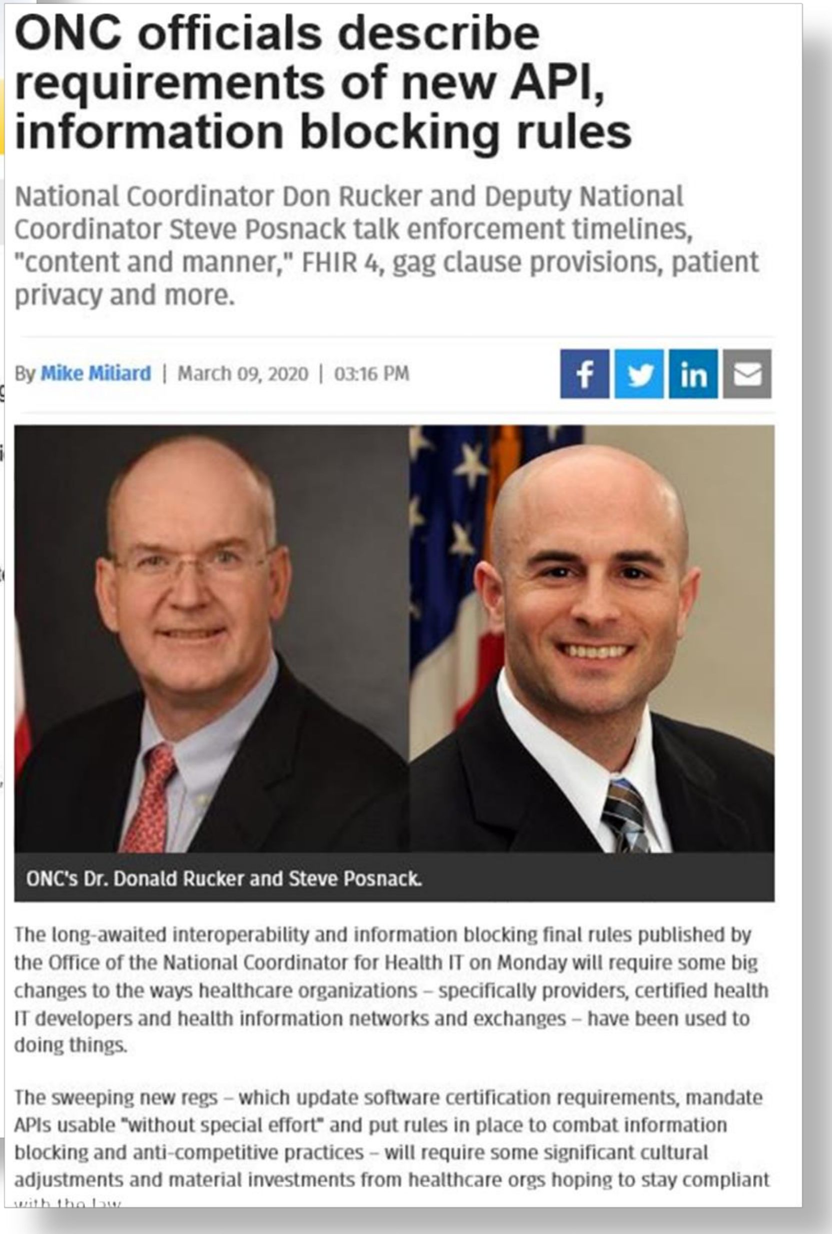
This rule finalizes new policies that give patients access to their health information and moves the healthcare system toward great interoperability. These new policies include:

- Patient Access API (*applicable January 1, 2021*)
- Provider Directory API (*applicable January 1, 2021*)
- Payer-to-Payer Data Exchange (*applicable January 1, 2022*)
- Improving the Dually Eligible Experience by Increasing the Frequency of Federal-State Data Exchanges (*applicable April 1, 2022*)
- Public Reporting and Information Blocking (*applicable late 2020*)
- Digital Contact Information (*applicable late 2020*)
- Admission, Discharge, and Transfer Event Notifications (*applicable fall 2020*)

Read the Fact Sheet to learn more about these new policies.

To view the CMS Interoperability and Patient Access final rule, download the PDF (PDF).

To view the ONC 21st Century Cures Act final rule, visit https://www.healthit.gov/curesrule.



ONC officials describe requirements of new API, information blocking rules

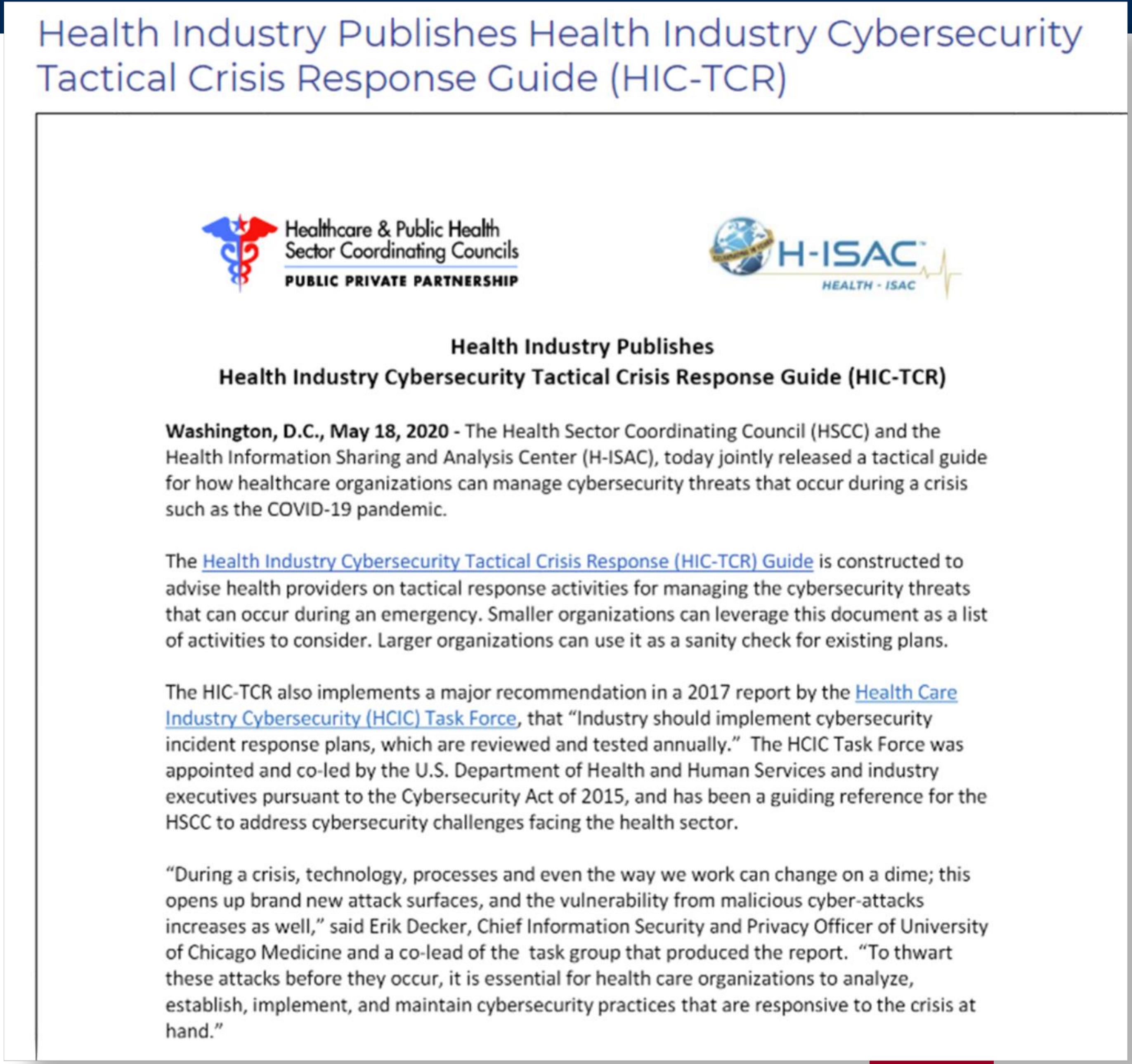
National Coordinator Don Rucker and Deputy National Coordinator Steve Posnack talk enforcement timelines, "content and manner," FHIR 4, gag clause provisions, patient privacy and more.

By Mike Miliard | March 09, 2020 | 03:16 PM

ONC's Dr. Donald Rucker and Steve Posnack.

The long-awaited interoperability and information blocking final rules published by the Office of the National Coordinator for Health IT on Monday will require some big changes to the ways healthcare organizations – specifically providers, certified health IT developers and health information networks and exchanges – have been used to doing things.

The sweeping new regs – which update software certification requirements, mandate APIs usable "without special effort" and put rules in place to combat information blocking and anti-competitive practices – will require some significant cultural adjustments and material investments from healthcare orgs hoping to stay compliant with the law.



Health Industry Publishes Health Industry Cybersecurity Tactical Crisis Response Guide (HIC-TCR)

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

H-ISAC
HEALTH - ISAC

Health Industry Publishes
Health Industry Cybersecurity Tactical Crisis Response Guide (HIC-TCR)

Washington, D.C., May 18, 2020 - The Health Sector Coordinating Council (HSCC) and the Health Information Sharing and Analysis Center (H-ISAC), today jointly released a tactical guide for how healthcare organizations can manage cybersecurity threats that occur during a crisis such as the COVID-19 pandemic.

The Health Industry Cybersecurity Tactical Crisis Response (HIC-TCR) Guide is constructed to advise health providers on tactical response activities for managing the cybersecurity threats that can occur during an emergency. Smaller organizations can leverage this document as a list of activities to consider. Larger organizations can use it as a sanity check for existing plans.

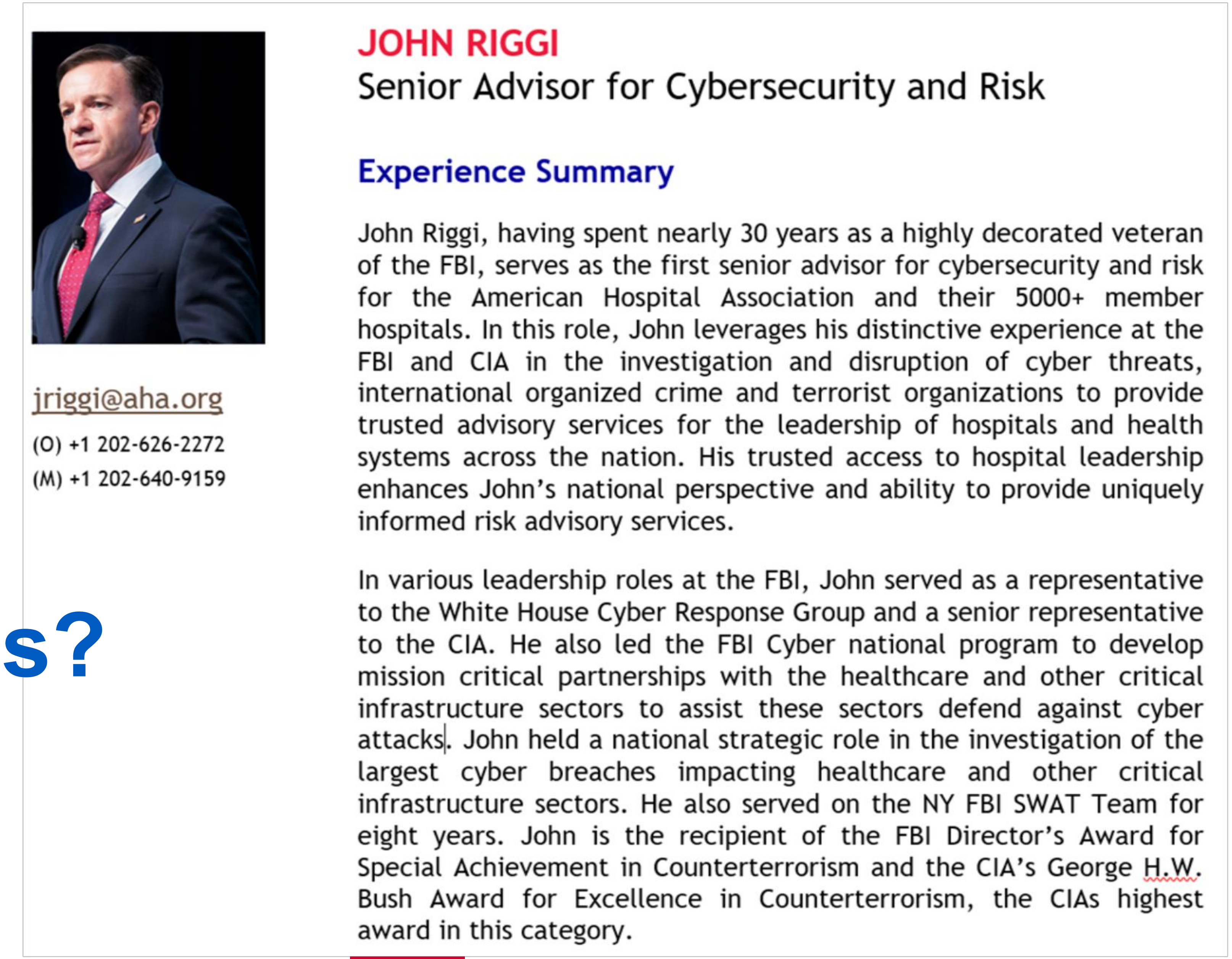
The HIC-TCR also implements a major recommendation in a 2017 report by the Health Care Industry Cybersecurity (HCIC) Task Force, that "Industry should implement cybersecurity incident response plans, which are reviewed and tested annually." The HCIC Task Force was appointed and co-led by the U.S. Department of Health and Human Services and industry executives pursuant to the Cybersecurity Act of 2015, and has been a guiding reference for the HSCC to address cybersecurity challenges facing the health sector.

"During a crisis, technology, processes and even the way we work can change on a dime; this opens up brand new attack surfaces, and the vulnerability from malicious cyber-attacks increases as well," said Erik Decker, Chief Information Security and Privacy Officer of University of Chicago Medicine and a co-lead of the task group that produced the report. "To thwart these attacks before they occur, it is essential for health care organizations to analyze, establish, implement, and maintain cybersecurity practices that are responsive to the crisis at hand."

https://healthsectorcouncil.org/health-industry-publishes-health-industry-cybersecurity-tactical-crisis-response-guide-hic-tcr/

American Hospital Association.

Questions?



JOHN RIGGI

Senior Advisor for Cybersecurity and Risk

jriggi@aha.org

(O) +1 202-626-2272

(M) +1 202-640-9159

Experience Summary

John Riggi, having spent nearly 30 years as a highly decorated veteran of the FBI, serves as the first senior advisor for cybersecurity and risk for the American Hospital Association and their 5000+ member hospitals. In this role, John leverages his distinctive experience at the FBI and CIA in the investigation and disruption of cyber threats, international organized crime and terrorist organizations to provide trusted advisory services for the leadership of hospitals and health systems across the nation. His trusted access to hospital leadership enhances John's national perspective and ability to provide uniquely informed risk advisory services.

In various leadership roles at the FBI, John served as a representative to the White House Cyber Response Group and a senior representative to the CIA. He also led the FBI Cyber national program to develop mission critical partnerships with the healthcare and other critical infrastructure sectors to assist these sectors defend against cyber attacks. John held a national strategic role in the investigation of the largest cyber breaches impacting healthcare and other critical infrastructure sectors. He also served on the NY FBI SWAT Team for eight years. John is the recipient of the FBI Director's Award for Special Achievement in Counterterrorism and the CIA's George H.W. Bush Award for Excellence in Counterterrorism, the CIAs highest award in this category.