Dear members and friends,

Reducing the cybersecurity risk to one of the most vulnerable aspects of commerce — *global supply chains* — is the goal of a new publication by the National Institute of Standards and Technology (NIST), whose computer security experts have distilled a set of effective risk management techniques into a draft guidebook for businesses. NIST is seeking public comment on the draft for the next 30 days.

The Key Practices in Cyber Supply Chain Risk Management, draft NISTIR 8276 - [https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8276-draft.pdf](https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8276-draft.pdf) provides a set of strategies to help businesses address the cybersecurity issues posed by modern information and communications technology products, which are commonly built using components and services supplied by third-party organizations.

The composed nature of these devices and systems makes them difficult to secure effectively against malware and other threats, placing manufacturers, service providers and end users at risk.

“The seed of the problem is that everything is interconnected nowadays,” said NIST’s Jon Boyens, one of the draft report’s authors. “Products are very sophisticated, and with our globalized economy, companies often outsource the tasks of developing components and code to other companies, involving multiple tiers of suppliers.”

Vulnerabilities in the cyber supply chain — really a complex network of connections rather than a single strand — involve not only microchips and
their internal code, but also the support software for a device and the other companies that have access to its components.

Put them all together, and it can be a daunting task to anticipate every systemic weakness that an adversary might exploit.

Many recent cyber breaches have been linked to supply chain risks. A recent high-profile attack from the second half of 2018, Operation ShadowHammer, is estimated to have affected up to a million users.

A 2013 attack by the Dragonfly group targeted companies with industrial control systems, such as those distributing energy within the U.S. This attack infected companies in critical industries with malware. Symantec's 2019 Internet Security Threat Report found supply chain attacks increased by 78 percent in 2018.

The NIST report is a high-level document intended to be easily understood and applied in managing these risks. Its core is a 27-page section outlining eight key practices that have proved to be useful, from establishing a formal risk management program to collaborating closely with key suppliers.

Each key practice is accompanied by a set of recommendations, and because each organization will have its own specific needs, the authors also include guidance on how to apply these recommendations.

Acknowledging that companies in different economic sectors might manage supply chain risk differently, the authors also offer a set of 24 case studies in risk management that feature a variety of businesses ranging from aerospace and IT manufacturers to consumer goods companies. These case studies, along with a summary of the findings, are available at NIST’s Cyber Supply Chain Risk Management Key Practices page.

“Many companies share the same suppliers, but their overall supply chains are still very different,” Boyens said. “To supplement our report you can look for the case studies that are relevant to your industry.”

The April 2018 update to the NIST Cybersecurity Framework added a new section about supply chain risk management, and the new report cross-references the framework so that organizations can use both sets of NIST guidance together, Boyens said.

Public comments on Draft NISTIR 8276 were submitted until March 4, 2020, to scrm-nist@nist.gov, and NIST will consider them before releasing a final version, planned for Spring 2020.
Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
NIST Special Publication 800-171, Revision 2

The protection of Controlled Unclassified Information (CUI) resident in nonfederal systems and organizations is of paramount importance to federal agencies and can directly impact the ability of the federal government to successfully conduct its essential missions and functions.

This publication provides agencies with recommended security requirements for protecting the confidentiality of CUI when the information is resident in nonfederal systems and organizations; when the nonfederal organization is not collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency; and where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or governmentwide policy for the CUI category listed in the CUI Registry.

The requirements apply to all components of nonfederal systems and organizations that process, store, and/or transmit CUI, or that provide protection for such components.

The security requirements are intended for use by federal agencies in contractual vehicles or other agreements established between those agencies and nonfederal organizations.

<table>
<thead>
<tr>
<th>TABLE 1: SECURITY REQUIREMENT FAMILIES</th>
</tr>
</thead>
<tbody>
<tr>
<td>FAMILY</td>
</tr>
<tr>
<td>Access Control</td>
</tr>
<tr>
<td>Awareness and Training</td>
</tr>
<tr>
<td>Audit and Accountability</td>
</tr>
<tr>
<td>Configuration Management</td>
</tr>
<tr>
<td>Identification and Authentication</td>
</tr>
<tr>
<td>Incident Response</td>
</tr>
<tr>
<td>Maintenance</td>
</tr>
</tbody>
</table>

The purpose of this publication is to provide federal agencies with recommended security requirements for protecting the confidentiality of CUI:
(1) when the CUI is resident in a nonfederal system and organization;

(2) when the nonfederal organization is not collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency; and

(3) where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or governmentwide policy for the CUI category listed in the CUI Registry.

The requirements apply only to components of nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components.

The requirements are intended for use by federal agencies in appropriate contractual vehicles or other agreements established between those agencies and nonfederal organizations. In CUI guidance and the CUI Federal Acquisition Regulation (FAR), the CUI Executive Agent will address determining compliance with security requirements.

To read more: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf
Financial markets and monetary policy - is there a hall of mirrors problem?

Richard H Clarida, Vice Chair of the Board of Governors of the Federal Reserve System, at the 2020 US Monetary Policy Forum, sponsored by the Initiative on Global Markets at the University of Chicago Booth School of Business, New York City.

Thank you to the conference organizers for inviting me here to discuss what former Chair Bernanke has famously referred to as a “hall of mirrors” problem: a situation in which a central bank’s reaction function and financial market prices interact in economically suboptimal and potentially destabilizing ways.

In my remarks today, I will lay out the way I think about the interplay between financial markets and monetary policy, with a focus on how I myself seek to integrate noisy but often correlated signals about the economy that I glean from models, surveys, and financial markets.

Three Observations

I begin with three unobjectionable observations.

First, because of Friedman’s long and variable lags, monetary policy should be—and, at the Fed, is—forward looking.

Policy decisions made today will have no effect on today’s inflation or unemployment rates, so good policy needs to assess where the economic fundamentals are going tomorrow to calibrate appropriate policy today.

Of course, financial markets are also forward looking.

An asset’s value today depends upon its expected future cash flows discounted by a rate that reflects the expected path of the policy rate plus an appropriate risk premium.

Thus, central banks and financial markets are looking at the same data on macro fundamentals to make inferences about the future path of the economy, and, of course, any decisions on the policy path made by the central bank will influence asset prices through the discount factor.
So optimal monetary policy will (almost) always be correlated with asset prices. Correlation is not evidence of causation, and the hall of mirrors problem at its essence is about inferring causation from correlation.

To read more:
https://www.bis.org/review/r200223b.pdf
The EU-U.S. Public Forum will take place at the premises of the U.S. Chamber of Commerce in Washington, DC.

**9:00 - 9:15 a.m.  Welcoming Remarks and Forum Objectives**
- Steven Seitz, Director, Federal Insurance Office
- Doug Ommen, Commissioner, Iowa Insurance Division
- Gabriel Bernardino, Chairman of the EIOPA Board of Supervisors

**9:15 - 10:15 a.m.  Panel 1 – Confronting Cross-Border Insurer Cybersecurity Risks**

Cyber risk continues to grow and evolve, both for the insurance industry itself and for the U.S. and EU markets and businesses served by insurers. This past year, the EU-US Insurance Project has examined cross-border cybersecurity incidents and how to coordinate responses to such incidents. This panel will address how the insurance industry and regulators can enhance insurance sector cybersecurity, including how best to continue and enhance cross-border coordination and information sharing among all stakeholders.

- **Moderator:** Steven Seitz, Federal Insurance Office, U.S. Department of the Treasury
- Jillian Froment, Director, Ohio Department of Insurance
- Petra Hieltema, Director Insurance Supervision, De Nederlandsche Bank (DNB)
- Kelly Ann Harris, Vice President, Corporate Counsel – Cybersecurity & Privacy, Prudential
- Neville Dunne, Chief Operating Officer, Zurich Insurance plc, Ireland

**10:30 – 11:30 a.m.  Panel 2 – Development of the Cyber Insurance Market: Challenges and Opportunities of Insuring and Reinsuring Cyber Risk**

This panel will discuss approaches for collecting data and developing techniques supporting more sophisticated assessment of cyber risks and potential accumulation risks. Taking into account the global character of cyber risks panelists will elaborate on whether globally harmonized standards could facilitate further understanding and underwriting of cyber risks. The discussion will further include the role and use of risk pools to provide additional capacity to tackle the potential systemic nature of cyber risk.

- **Moderator:** Gabriel Bernardino, Chairman of the EIOPA Board of Supervisors
- Jillian Froment, Director, Ohio Department of Insurance
- Dr. Frank Grund, Chief Executive Director of Insurance and Pension Supervision, Federal Financial Supervisory Authority, Germany
- Matthew McCabe, Senior Vice President, Marsh USA, Inc.
- Joshua Motta, CEO, Coalition, Inc.
- Giles Taylor, Chief Risk and Compliance Officer, Lloyd’s Brussels
Panelists will discuss insurers’ use of third-party vendors and how the regulatory framework addresses big data accuracy and new vendors operating in the insurance marketplace. Panelists will also discuss privacy protections and disclosures to applicants and policyholders. Panelists will explore the associated opportunities and risks of insurers’ use of AI and corresponding regulatory responses in the US and EU, such as the development of AI principles including ethical aspects. Finally, panelists will discuss the regulatory review of predictive models, including but not limited to assessing transparency and explainability issues arising from the use of ML algorithms.

- **Moderator:** Jillian Froment, Director, Ohio Department of Insurance
- **Doug Ommen,** Commissioner, Iowa Insurance Division
- **Domhnall Cullinan**, Director of Insurance Supervision, Central Bank of Ireland
- **Timothy Jones,** Chief Innovation Officer, Transamerica
- **Peter Kochenburger,** Deputy Director of the Insurance Law Center and Associate Clinical Professor of Law at the University of Connecticut School of Law
- **Marcin Detyniecki,** Group Chief Data Scientist and Head of R&D, AXA Group

The public event will include discussions of key areas linked to the Project initiatives addressing challenges and opportunities for the insurance sector in the European Union and the United States related to cyber security risks and the cyber insurance market, and the use of big data.

Representatives of the European Commission (EC), European Insurance and Occupational Pensions Authority (EIOPA), the Federal Insurance Office of the U.S. Department of the Treasury (FIO) and the National Association of Insurance Commissioners (NAIC), will lead the Forum. Other EU and US authorities will also participate in this event.

Panel sessions will include discussions amongst regulators, industry and consumer representatives on approaches, practices and solutions addressing the multi-fold challenges, risks and opportunities regarding these covered topics.

The Programme is available at: [https://www.eiopa.europa.eu/content/agenda-eu-us-insurance-project-public-forum-13-march-2020-washington](https://www.eiopa.europa.eu/content/agenda-eu-us-insurance-project-public-forum-13-march-2020-washington)
Alert (AA20-049A)
Ransomware Impacting Pipeline Operations
Cybersecurity and Infrastructure Security Agency (CISA)

The Cybersecurity and Infrastructure Security Agency (CISA) encourages asset owner operators across all critical infrastructure sectors to review the below threat actor techniques and ensure the corresponding mitigations are applied.

CISA responded to a cyberattack affecting control and communication assets on the operational technology (OT) network of a natural gas compression facility.

A cyber threat actor used a Spearphishing Link [https://attack.mitre.org/techniques/T1192/] to obtain initial access to the organization’s information technology (IT) network before pivoting to its OT network.

The threat actor then deployed commodity ransomware to Encrypt Data for Impact on both networks. Specific assets experiencing a Loss of Availability on the OT network included human machine interfaces (HMIs), data historians, and polling servers.

Impacted assets were no longer able to read and aggregate real-time operational data reported from low-level OT devices, resulting in a partial Loss of View for human operators.

The attack did not impact any programmable logic controllers (PLCs) and at no point did the victim lose control of operations.

Although the victim’s emergency response plan did not specifically consider cyberattacks, the decision was made to implement a deliberate and controlled shutdown to operations.

This lasted approximately two days, resulting in a Loss of Productivity and Revenue, after which normal operations resumed.

CISA is providing this Alert to help administrators and network defenders protect their organizations against this and similar ransomware attacks.
Network and Assets

- The victim failed to implement robust segmentation between the IT and OT networks, which allowed the adversary to traverse the IT-OT boundary and disable assets on both networks.

- The threat actor used commodity ransomware to compromise Windows-based assets on both the IT and OT networks. Assets impacted on the organization’s OT network included HMIs, data historians, and polling servers.

- Because the attack was limited to Windows-based systems, PLCs responsible for directly reading and manipulating physical processes at the facility were not impacted.

- The victim was able to obtain replacement equipment and load last-known-good configurations to facilitate the recovery process.

- All OT assets directly impacted by the attack were limited to a single geographic facility.

To read more: https://www.us-cert.gov/ncas/alerts/aa20-049a
Preliminary Report on Foreign Holdings of U.S. Securities at End-June 2019


Final survey results, which will include additional detail as well as possible revisions to the preliminary data, will be reported on April 30, 2020.

The survey was undertaken jointly by Treasury, the Federal Reserve Bank of New York, and the Board of Governors of the Federal Reserve System.

The next annual survey will cover holdings at the end of June 2020; preliminary data are expected to be released by February 26, 2021.

Complementary surveys measuring U.S. holdings of foreign securities are also carried out annually. Data from the most recent survey, reporting on securities held at year-end 2019, are currently being processed. Preliminary results are expected to be reported by August 31, 2020.

Table A. Foreign holdings of U.S. securities, by type of security, as of recent survey dates

(Billions of dollars)

<table>
<thead>
<tr>
<th>Type of security</th>
<th>June 30, 2018</th>
<th>June 30, 2019</th>
</tr>
</thead>
<tbody>
<tr>
<td>Long-term securities</td>
<td>18,421</td>
<td>19,935</td>
</tr>
<tr>
<td>Equities</td>
<td>8,139</td>
<td>8,899</td>
</tr>
<tr>
<td>Long-term debt</td>
<td>10,282</td>
<td>11,035</td>
</tr>
<tr>
<td>Asset-backed</td>
<td>1,317</td>
<td>1,447</td>
</tr>
<tr>
<td>Other</td>
<td>8,965</td>
<td>9,589</td>
</tr>
<tr>
<td>Short-term debt securities</td>
<td>980</td>
<td>924</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>19,400</strong></td>
<td><strong>20,858</strong></td>
</tr>
<tr>
<td>Of which: Official</td>
<td>5,794</td>
<td>6,116</td>
</tr>
</tbody>
</table>

The survey measured the value of foreign holdings of U.S. securities as of June 30, 2019, to be **$20,858 billion**, with $8,899 billion held in U.S. equities, $11,035 billion held in U.S. long-term debt securities (of which $1,447 billion are holdings of asset-backed securities (ABS) and $9,589...
billion are holdings of non-ABS securities), and $924 billion held in U.S. short-term debt securities.

The previous survey, conducted as of June 30, 2018, measured the value of total foreign holdings of U.S. securities at **$19,400 billion**, with holdings of $8,139 billion in U.S. equities, $10,282 billion in U.S. long-term debt securities, and $980 billion in U.S. short-term debt securities.

### Table B. Foreign holdings of U.S. securities, by country and type of security, for the major investing countries into the U.S., as of June 30, 2019

<table>
<thead>
<tr>
<th>Country</th>
<th>Total (Billions)</th>
<th>Equities (Billions)</th>
<th>Long-term Debt (Billions)</th>
<th>Short-term (Billions)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Total</td>
<td>Equities</td>
<td>ABS</td>
<td>Other</td>
</tr>
<tr>
<td>Japan</td>
<td>2,360</td>
<td>652</td>
<td>337</td>
<td>1,310</td>
</tr>
<tr>
<td>Cayman Islands</td>
<td>1,881</td>
<td>1,087</td>
<td>124</td>
<td>571</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>1,856</td>
<td>1,078</td>
<td>22</td>
<td>695</td>
</tr>
<tr>
<td>Luxembourg</td>
<td>1,629</td>
<td>663</td>
<td>84</td>
<td>791</td>
</tr>
<tr>
<td>China, mainland (2)</td>
<td>1,544</td>
<td>90</td>
<td>225</td>
<td>1,125</td>
</tr>
<tr>
<td>Canada</td>
<td>1,262</td>
<td>956</td>
<td>35</td>
<td>254</td>
</tr>
<tr>
<td>Ireland</td>
<td>1,085</td>
<td>456</td>
<td>73</td>
<td>448</td>
</tr>
<tr>
<td>Switzerland</td>
<td>823</td>
<td>450</td>
<td>29</td>
<td>303</td>
</tr>
<tr>
<td>Belgium</td>
<td>781</td>
<td>58</td>
<td>11</td>
<td>685</td>
</tr>
<tr>
<td>Taiwan</td>
<td>627</td>
<td>68</td>
<td>267</td>
<td>288</td>
</tr>
<tr>
<td>Norway</td>
<td>452</td>
<td>309</td>
<td>*</td>
<td>143</td>
</tr>
<tr>
<td>Netherlands</td>
<td>422</td>
<td>285</td>
<td>17</td>
<td>116</td>
</tr>
<tr>
<td>Singapore</td>
<td>415</td>
<td>232</td>
<td>7</td>
<td>164</td>
</tr>
<tr>
<td>Germany</td>
<td>398</td>
<td>193</td>
<td>19</td>
<td>176</td>
</tr>
<tr>
<td>Hong Kong</td>
<td>397</td>
<td>110</td>
<td>13</td>
<td>244</td>
</tr>
</tbody>
</table>
Helping to Protect the US 2020 Election

This overview provides a look at Facebook’s comprehensive efforts over the past three years to help protect the democratic process ahead of the 2020 US elections.

We know that elections have changed, and so has Facebook.

We’ve worked to develop a comprehensive strategy to close previous vulnerabilities while addressing new and emerging threats.

And we’ve developed smarter tools, greater transparency, and stronger partnerships to help us do just that.

We have more than 35,000 people dedicated to safety and security issues, with about 40 teams contributing to our work on elections.

We block millions of fake accounts each day so they can’t spread misinformation.

We continue to improve our coordination and cooperation with law enforcement, including DNI, DHS, FBI, as well as other federal officials, state election officials, and technology companies, to support better information sharing and threat detection in service of public safety.

And we’ve set a new standard for transparency in Pages and political ads so people can see who is behind them.

In 2016, we were on the lookout for traditional cyber threats like hacking and stealing information.

What happened was a much different kind of attack, meant to sow social discord around divisive political issues.

We’ve learned lessons from 2016 and while we have seen threats evolve, we’re working hard to stay ahead of those efforts so it’s harder to use our platform for election interference.

We know that security is never finished and we can’t do this alone— that’s why we continue to work with policymakers and experts to make sure we are constantly improving.
Rise in the number of Office 365 phishing scams

Cyber security researchers have uncovered an increase in the number of low-quality phishing scams that aim to trick users into revealing their credentials.

According to a new report from Cofense, there has been a surge in scam attempts using illegitimate and badly created Office 365 credentials update forms. The report: [https://cofense.com/phishers-using-google-forms-bypass-popular-email-gateways/](https://cofense.com/phishers-using-google-forms-bypass-popular-email-gateways/)

Potential victims receive an email claiming to be from their organisation’s IT team that tells them their account will expire unless they click the link and update their details.

Cofense note that the criminals behind the scam went to great lengths to appear legitimate. The phishing email originates from a compromised company email account, which allows the scam to bypass basic email security checks.

However, the forms that potential victims are directed to are often littered with grammatical and spelling mistakes.

Phishers use a wide variety of techniques to try and scam users into revealing sensitive data about themselves or the businesses they work for. The NCSC has published guidance on how the public and organisations can defend themselves against such attacks.

The NCSC has also published advice on securely configuring Office 365 to protect against the rise in credential stealing attacks at: [https://www.ncsc.gov.uk/blog-post/securing-office-365-with-better-configuration](https://www.ncsc.gov.uk/blog-post/securing-office-365-with-better-configuration)
CISA INSIGHTS
Risk Management for Novel Coronavirus (COVID-19)

The Threat and How to Think About It

This product is for executives to help them think through physical, supply chain, and cybersecurity issues that may arise from the spread of Novel Coronavirus, or COVID-19.

According to the U.S. Centers for Disease Control and Prevention (CDC), COVID-19 has been detected in locations around the world, including multiple areas throughout the U.S. This is a rapidly evolving situation and for more information, visit the CDC’s COVID-19 Situation Summary.

To read more:

Online training as a weapon to fight the new coronavirus

The learning team of the WHO Health Emergencies Programme worked with technical experts to quickly develop and publish the online course – you may visit: https://openwho.org/courses/introduction-to-ncov

Approximately 3000 new users have registered for the training every day since its launch, demonstrating the high level of interest in the virus among health professionals and the general public.

In addition, more than 200 000 people have viewed the introductory video to the course on YouTube.

The high engagement levels emerged as the international community launched a US$675 million preparedness and response plan to fight further spread of the new coronavirus and protect states with weaker health systems.

The free learning resource is available to anyone interested in novel coronavirus on WHO’s open learning platform for emergencies, OpenWHO.org.

The platform was established 3 years ago with emergencies such as nCoV in mind, in which WHO would need to reach millions of people across the globe with real-time, accessible learning materials.
The online training – entitled “Emerging respiratory viruses, including nCoV: methods for detection, prevention, response and control” – is currently being produced in all official UN languages and Portuguese.

“Our job is to work with technical health experts to package knowledge using adult learning principles, quickly so that it is most useful to health workers and our staff,” said Heini Utunen, who manages OpenWHO for the WHO Health Emergencies Programme (WHE).

“Our online platform – OpenWHO – is already accessed by users from every country on earth, providing more than 60 courses in 21 languages. Delivering trainings in the local language of responders is really important, especially in an emergency”.

WHE has been investing in learning and training to strengthen preparedness and real-time response to health emergencies.

The programme developed its first-ever learning strategy in 2018 and has a small dedicated Learning and Capacity Development Unit that allows WHE to develop trainings quickly and get know-how to those who most need it at the front line.

For the latest information on the new coronavirus, visit the 2019-nCoV page.
Interim Guidance for Businesses and Employers

This interim guidance is based on what is currently known about the coronavirus disease 2019 (COVID-19). The Centers for Disease Control and Prevention (CDC) will update this interim guidance as needed and as additional information becomes available.

The following interim guidance may help prevent workplace exposures to acute respiratory illnesses, including COVID-19, in non-healthcare settings. The guidance also provides planning considerations if there are more widespread, community outbreaks of COVID-19.

Recommended strategies for employers to use now:

1. Actively encourage sick employees to stay home:
   - Employees who have symptoms of acute respiratory illness are recommended to stay home and not come to work until they are free of fever (100.4°F [37.8°C] or greater using an oral thermometer), signs of a fever, and any other symptoms for at least 24 hours, without the use of fever-reducing or other symptom-altering medicines (e.g. cough suppressants). Employees should notify their supervisor and stay home if they are sick.
   - Ensure that your sick leave policies are flexible and consistent with public health guidance and that employees are aware of these policies.
   - Talk with companies that provide your business with contract or temporary employees about the importance of sick employees staying home and encourage them to develop non-punitive leave policies.
   - Do not require a healthcare provider’s note for employees who are sick with acute respiratory illness to validate their illness or to return to work, as healthcare provider offices and medical facilities may be extremely busy and not able to provide such documentation in a timely way.
   - Employers should maintain flexible policies that permit employees to stay home to care for a sick family member. Employers should be aware that more employees may need to stay at home to care for sick children or other sick family members than is usual.
2. *Separate sick employees:*

CDC recommends that employees who appear to have acute respiratory illness symptoms (i.e. cough, shortness of breath) upon arrival to work or become sick during the day should be separated from other employees and be sent home immediately. Sick employees should cover their noses and mouths with a tissue when coughing or sneezing (or an elbow or shoulder if no tissue is available).

3. *Emphasize staying home when sick, respiratory etiquette and hand hygiene by all employees:*

- Place posters that encourage staying home when sick, cough and sneeze etiquette, and hand hygiene at the entrance to your workplace and in other workplace areas where they are likely to be seen.

- Provide tissues and no-touch disposal receptacles for use by employees.

- Instruct employees to clean their hands often with an alcohol-based hand sanitizer that contains at least 60-95% alcohol, or wash their hands with soap and water for at least 20 seconds. Soap and water should be used preferentially if hands are visibly dirty.

- Provide soap and water and alcohol-based hand rubs in the workplace. Ensure that adequate supplies are maintained. Place hand rubs in multiple locations or in conference rooms to encourage hand hygiene.

- Visit the coughing and sneezing etiquette and clean hands webpage for more information.

4. *Perform routine environmental cleaning:*

- Routinely clean all frequently touched surfaces in the workplace, such as workstations, countertops, and doorknobs. Use the cleaning agents that are usually used in these areas and follow the directions on the label.

- No additional disinfection beyond routine cleaning is recommended at this time.

- Provide disposable wipes so that commonly used surfaces (for example, doorknobs, keyboards, remote controls, desks) can be wiped down by employees before each use.

5. *Advise employees before traveling to take certain steps:*
- Check the CDC’s Traveler’s Health Notices for the latest guidance and recommendations for each country to which you will travel. Specific travel information for travelers going to and returning from China, and information for aircrew, can be found at on the CDC website.

- Advise employees to check themselves for symptoms of acute respiratory illness before starting travel and notify their supervisor and stay home if they are sick.

- Ensure employees who become sick while traveling or on temporary assignment understand that they should notify their supervisor and should promptly call a healthcare provider for advice if needed.

- If outside the United States, sick employees should follow your company’s policy for obtaining medical care or contact a healthcare provider or overseas medical assistance company to assist them with finding an appropriate healthcare provider in that country. A U.S. consular officer can help locate healthcare services. However, U.S. embassies, consulates, and military facilities do not have the legal authority, capability, and resources to evacuate or give medicines, vaccines, or medical care to private U.S. citizens overseas.

6. Additional Measures in Response to Currently Occurring Sporadic Importations of the COVID-19:

- Employees who are well but who have a sick family member at home with COVID-19 should notify their supervisor and refer to CDC guidance for how to conduct a risk assessment of their potential exposure.

- If an employee is confirmed to have COVID-19, employers should inform fellow employees of their possible exposure to COVID-19 in the workplace but maintain confidentiality as required by the Americans with Disabilities Act (ADA). Employees exposed to a co-worker with confirmed COVID-19 should refer to CDC guidance for how to conduct a risk assessment of their potential exposure.

The severity of illness or how many people will fall ill from COVID-19 is unknown at this time. If there is evidence of a COVID-19 outbreak in the U.S., employers should plan to be able to respond in a flexible way to varying levels of severity and be prepared to refine their business response plans as needed.

For the general American public, such as workers in non-healthcare settings and where it is unlikely that work tasks create an increased risk of exposures to COVID-19, the immediate health risk from COVID-19 is considered low.
The CDC and its partners will continue to monitor national and international data on the severity of illness caused by COVID-19, will disseminate the results of these ongoing surveillance assessments, and will make additional recommendations as needed.

Critical Infrastructure Protection, Additional Actions Needed to Identify Framework Adoption and Resulting Improvements

Abbreviations

ASPR - Assistant Secretary for Preparedness and Response
DHS - Department of Homeland Security
DOD - Department of Defense
DOT - Department of Transportation
EPA - Environmental Protection Agency
GSA - General Services Administration
HHS - Department of Health and Human Services
ISAC - Information Sharing and Analysis Center
ISO - International Organization for Standardization
IT - information technology
NIST - National Institute of Standards and Technology
SCC - Sector Coordinating Council
SSA - Sector Specific Agency

Conclusions

Most of the SSAs have not determined the level and type of framework adoption, as we previously recommended. Most of the sectors, however, had efforts underway to encourage and facilitate use of the framework. Even with this progress, implementation of our recommendations is essential to the success of protection efforts.

While selected organizations reported varying levels of improvements, the SSAs have not collected and reported sector-wide improvements as a result of framework use.

The SSAs and organizations identified impediments to collecting and reporting sector-wide improvements, including the lack of precise measurements of improvement, voluntary nature of the framework, and lack of a centralized information sharing mechanism.

However, NIST and DHS have initiatives to help address these impediments.

These included an information security measurement program, cybersecurity framework starter profile, information sharing programs, self-assessment tools, and surveys to support SSAs in measuring and quantifying improvements in the protection of critical
infrastructure as a result of using the framework.

However, NIST has yet to establish time frames for completing the information security measurement program and starter profile.

Moreover, the SSAs have yet to report on sector-wide improvements using the initiatives.

Until they do so, the critical infrastructure sectors may not fully understand the value of the framework to better protect their critical infrastructures from cyber threats.

**Recommendations**

We are making the following 10 recommendations to NIST and the nine sector-specific agencies.

The Director of NIST should establish time frames for completing NIST’s initiatives, to include the information security measurement program and the cybersecurity framework starter profile, to enable the identification of sector-wide improvements from using the framework in the protection of critical infrastructure from cyber threats. (Recommendation 1).

The Secretary of Agriculture, in coordination with the Secretary of Health and Human Services, should take steps to consult with respective sector partner(s), such as the SCC, DHS, and NIST, as appropriate, to collect and report sector-wide improvements from use of the framework across its critical infrastructure sector using existing initiatives. (Recommendation 2).

The Secretary of Defense should take steps to consult with respective sector partner(s), such as the SCC, DHS, and NIST, as appropriate, to collect and report sector-wide improvements from use of the framework across its critical infrastructure sector using existing initiatives. (Recommendation 3).

The Secretary of Energy should take steps to consult with respective sector partner(s), such as the SCC, DHS, and NIST, as appropriate, to collect and report sector-wide improvements from use of the framework across its critical infrastructure sector using existing initiatives. (Recommendation 4).

The Administrator of the Environmental Protection Agency should take steps to consult with respective sector partner(s), such as the SCC, DHS, and NIST, as appropriate, to collect and report sector-wide improvements from use of the framework across its critical infrastructure sector using existing initiatives. (Recommendation 5).
The Administrator of the General Services Administration, in coordination with the Secretary of Homeland Security, should take steps to consult with respective sector partner(s), such as the Coordinating Council and NIST, as appropriate, to collect and report sector-wide improvements from use of the framework across its critical infrastructure sector using existing initiatives. (Recommendation 6).

The Secretary of Health and Human Services, in coordination with the Secretary of Agriculture, should take steps to consult with respective sector partner(s), such as the SCC, DHS, and NIST, as appropriate, to collect and report sector-wide improvements from use of the framework across its critical infrastructure sector using existing initiatives. (Recommendation 7).

The Secretary of Homeland Security should take steps to consult with respective sector partner(s), such as the SCC and NIST, as appropriate, to collect and report sector-wide improvements from use of the framework across its critical infrastructure sectors using existing initiatives. (Recommendation 8).

The Secretary of Transportation, in coordination with the Secretary of Homeland Security, should take steps to consult with respective sector partner(s) such as the SCC and NIST, as appropriate, to collect and report sector-wide improvements from use of the framework across its critical infrastructure sector using existing initiatives. (Recommendation 9).

The Secretary of the Treasury should take steps to consult with respective sector partner(s), such as the SCC, DHS, and NIST, as appropriate, to collect and report sector-wide improvements from use of the framework across its critical infrastructure sector using existing initiatives. (Recommendation 10).

The report:
**Figure 1: Critical Infrastructure Sectors and Related Sector-Specific Agencies**

<table>
<thead>
<tr>
<th>Sector-specific agency</th>
<th>Agency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chemical</td>
<td>DHS</td>
</tr>
<tr>
<td>Consists of institutions, such as commercial banks, credit unions, insurance companies, mutual funds, government-sponsored enterprises, pension funds, and other financial institutions that carry out financial transactions.</td>
<td></td>
</tr>
<tr>
<td>Commercial facilities</td>
<td>DHS</td>
</tr>
<tr>
<td>Protects sites where large numbers of people congregate, such as commercial centers, office buildings, sports stadiums, and theme parks.</td>
<td></td>
</tr>
<tr>
<td>Communications</td>
<td>DHS</td>
</tr>
<tr>
<td>Delivers wired, wireless, and satellite communications to meet the needs of business and governments.</td>
<td></td>
</tr>
<tr>
<td>Critical manufacturing</td>
<td>DHS</td>
</tr>
<tr>
<td>Alters materials into finished goods, to include manufacture of primary metals, machinery, electrical equipment, appliances and components, and transportation equipment.</td>
<td></td>
</tr>
<tr>
<td>Dams</td>
<td>DHS</td>
</tr>
<tr>
<td>Provides support to water retention structures, including levees, dams, navigation locks, canals, and larger and nationally symbolic dams that are major components of other critical infrastructures that provide electricity and water.</td>
<td></td>
</tr>
<tr>
<td>Defense industrial base</td>
<td>DOD</td>
</tr>
<tr>
<td>Supplies the military with the resources to protect the nation by producing weapons, aircraft, and ships, and provides essential services, including information technology and supply and maintenance.</td>
<td></td>
</tr>
<tr>
<td>Emergency services</td>
<td>DHS</td>
</tr>
<tr>
<td>Protects lives and property from accidents and disaster. This sector includes fire, rescue, emergency medical services, and law enforcement organizations.</td>
<td></td>
</tr>
<tr>
<td>Energy</td>
<td>DOE</td>
</tr>
<tr>
<td>Delivers the electric power used by all sectors and also includes the refining, storage, and distribution of oil and gas. The sector is divided into electricity and oil and natural gas.</td>
<td></td>
</tr>
<tr>
<td>Financial services</td>
<td>TREASURY</td>
</tr>
<tr>
<td>Ensures the safety and security of food, animal feed, and food-producing animals; coordinates animal and plant disease and pest response; and provides nutritional assistance.</td>
<td></td>
</tr>
<tr>
<td>Food and agriculture</td>
<td>USDA</td>
</tr>
<tr>
<td>Ensures continuity of functions for facilities owned and leased by the government, including all federal, state, territorial, local, and tribal government facilities located in the United States and abroad.</td>
<td></td>
</tr>
<tr>
<td>Government facilities</td>
<td>GSA</td>
</tr>
<tr>
<td>Protects the health of the population in the event of a disaster or attack. The sector consists of direct healthcare, health plans and payers, pharmaceuticals, laboratories, blood, medical materials, health information technology, mortuary care, and public health.</td>
<td></td>
</tr>
<tr>
<td>Healthcare and public health</td>
<td>HHS</td>
</tr>
<tr>
<td>Provides information technology, to include hardware manufacturers, software developers, and service providers, as well as the internet as a key resource.</td>
<td></td>
</tr>
<tr>
<td>Information technology</td>
<td>DHS</td>
</tr>
<tr>
<td>Provides nuclear power and materials. The sector includes commercial and research nuclear reactors; nuclear fuel fabrication facilities; reactor decommissioning; and the transportation, storage, and disposal of nuclear materials and waste.</td>
<td></td>
</tr>
<tr>
<td>Nuclear reactor, materials, and waste</td>
<td>DHS</td>
</tr>
<tr>
<td>Provides efficient, safe, and secure freedom of movement for people and commerce across the Nation’s transportation systems (aviation, freight rail, highways, maritime, mass transit, motor carriers, pipelines, and postal and shipping).</td>
<td></td>
</tr>
<tr>
<td>Transportation systems</td>
<td>DOT</td>
</tr>
<tr>
<td>Provides sources of safe drinking water from community water systems and properly treated wastewater from publicly owned treatment works.</td>
<td></td>
</tr>
<tr>
<td>Water and wastewater systems</td>
<td>EPA</td>
</tr>
</tbody>
</table>

Camouflage for the Digital Domain  
NATO STRATCOM COE

Discoverability of geolocation

Protecting the geolocation of personnel, equipment, infrastructure, and installations of military units is crucial for mission success.

Today’s digitalised society generates an abundance of open information that an adversary can exploit to obtain sensitive geolocation information.

While geolocation information is easily accessed using digital sources, it can also be provided directly by conflict participants and the general public via digital platforms.

Geolocation data allows an adversary to discover and adapt to the position and movements of forces, thus serving as a tactical, operational, or strategic force multiplier.

It also often enables or improves kinetic targeting and battle damage assessments. Geolocation data can also be useful information for enemy influence activities against friendly forces.

The paper:  
https://www.stratcomcoe.org/camouflage-digital-domain
Covid-19 and SARS: what do stock markets tell us?

The rapid spread of Covid-19 since mid-January invariably brings up a comparison with the early 2003 outbreak of severe acute respiratory syndrome (SARS).

In this box, we provide a preliminary assessment of the relative impact of the Covid-19 and SARS epidemics on various economies through the lens of equity investors.

An advantage of looking at the stock markets of different countries is that equity valuations should encompass both the local and global risk factors that the investors view as important.

Fluctuations in the global risk factor - gauged, for instance, through the returns on the MSCI Global index - may be driven by investors' concerns about the global economic fallout of a virus outbreak.
Such fluctuations are likely to have a differential effect on each country’s stock market performance; moreover, the magnitude of these effects is likely to have changed in the nearly two decades between the two epidemics.

Nevertheless, we can calculate "idiosyncratic" stock returns, the portion of a country-specific stock return that is not explained by fluctuations in the global risk factor, as the residual from a regression of the country's returns on the returns on the MSCI Global index.

The comparison of the idiosyncratic country-specific returns during periods in which the Covid-19 and SARS epidemics unfolded can thus provide a cleaner assessment of the relative fallouts from the two outbreaks across countries and time, at least as perceived by equity investors.

To read more: https://www.bis.org/publ/qtrpdf/r_qt2003w.htm
New action to disrupt world’s largest online criminal network
Tom Burt - Corporate Vice President, Customer Security & Trust

Microsoft and partners across 35 countries took coordinated legal and technical steps to disrupt one of the world’s most prolific botnets, called Necurs, which has infected more than nine million computers globally.

This disruption is the result of eight years of tracking and planning and will help ensure the criminals behind this network are no longer able to use key elements of its infrastructure to execute cyberattacks.

A botnet is a network of computers that a cybercriminal has infected with malicious software, or malware.

Once infected, criminals can control those computers remotely and use them to commit crimes.

Microsoft’s Digital Crimes Unit, BitSight and others in the security community first observed the Necurs botnet in 2012 and have seen it distribute several forms of malware, including the GameOver Zeus banking trojan.

The Necurs botnet is one of the largest networks in the spam email threat ecosystem, with victims in nearly every country in the world.

During a 58-day period in our investigation, for example, we observed that one Necurs-infected computer sent a total of 3.8 million spam emails to over 40.6 million potential victims.

Necurs is believed to be operated by criminals based in Russia and has also been used for a wide range of crimes including pump-and-dump stock scams, fake pharmaceutical spam email and “Russian dating” scams.

It has also been used to attack other computers on the internet, steal credentials for online accounts, and steal people’s personal information and confidential data.

Interestingly, it seems the criminals behind Necurs sell or rent access to the infected computer devices to other cybercriminals as part of a botnet-for-hire service.

Necurs is also known for distributing financially targeted malware and ransomware, cryptomining, and even has a DDoS (distributed denial of service) capability that has not yet been activated but could be at any moment.
On Thursday, March 5, the U.S. District Court for the Eastern District of New York issued an order enabling Microsoft to take control of U.S.-based infrastructure Necurs uses to distribute malware and infect victim computers.

With this legal action and through a collaborative effort involving public-private partnerships around the globe, Microsoft is leading activities that will prevent the criminals behind Necurs from registering new domains to execute attacks in the future.

This was accomplished by analyzing a technique used by Necurs to systematically generate new domains through an algorithm.

We were then able to accurately predict over six million unique domains that would be created in the next 25 months.

Microsoft reported these domains to their respective registries in countries around the world so the websites can be blocked and thus prevented from becoming part of the Necurs infrastructure. By taking control of existing websites and inhibiting the ability to register new ones, we have significantly disrupted the botnet.

Microsoft is also taking the additional step of partnering with Internet Service Providers (ISPs) and others around the world to rid their customers’ computers of malware associated with the Necurs botnet.

This remediation effort is global in scale and involves collaboration with partners in industry, government and law enforcement via the Microsoft Cyber Threat Intelligence Program (CTIP).

Through CTIP, Microsoft provides law enforcement, government Computer Emergency Response Teams (CERTs), ISPs and government agencies responsible for the enforcement of cyber laws and the protection of critical infrastructure with better insights into criminal cyber infrastructure located within their jurisdiction, as well as a view of compromised computers and victims impacted by such criminal infrastructure.

For this disruption, we are working with ISPs, domain registries, government CERTs and law enforcement in Mexico, Colombia, Taiwan, India, Japan, France, Spain, Poland and Romania, among others. Each of us has a critical role to play in protecting customers and keeping the internet safe.

To make sure your computer is free of malware, you may visit: https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/safety-scanner-download
The Cyberspace Solarium Commission (CSC) was established in the John S. McCain National Defense Authorization Act for Fiscal Year 2019 to "develop a consensus on a strategic approach to defending the United States in cyberspace against cyberattacks of significant consequences."

The finished report was presented to the public on March 11, 2020.
The Cyberspace Solarium Commission's proposes a strategy of layered cyber deterrence. The report consists of over 80 recommendations to implement the strategy.

These recommendations are organized into 6 pillars:

4. Reshape the Cyber Ecosystem.
5. Operationalize Cybersecurity Collaboration with the Private Sector.

To read more:
https://drive.google.com/file/d/1ryMCIL_dZ3oQyjFqFkkf10MxIXJGT4yy/view
Disclaimer

The Association tries to enhance public access to information about risk and compliance management.

Our goal is to keep this information timely and accurate. If errors are brought to our attention, we will try to correct them.

This information:

- is of a general nature only and is not intended to address the specific circumstances of any particular individual or entity;

- should not be relied on in the particular context of enforcement or similar regulatory action;

- is not necessarily comprehensive, complete, or up to date;

- is sometimes linked to external sites over which the Association has no control and for which the Association assumes no responsibility;

- is not professional or legal advice (if you need specific advice, you should always consult a suitably qualified professional);

- is in no way constitutive of an interpretative document;

- does not prejudge the position that the relevant authorities might decide to take on the same matters if developments, including Court rulings, were to lead it to revise some of the views expressed here;

- does not prejudge the interpretation that the Courts might place on the matters at issue.

Please note that it cannot be guaranteed that these information and documents exactly reproduce officially adopted texts.

It is our goal to minimize disruption caused by technical errors. However, some data or information may have been created or structured in files or formats that are not error-free and we cannot guarantee that our service will not be interrupted or otherwise affected by such problems.

The Association accepts no responsibility with regard to such problems incurred as a result of using this site or any linked external sites.
Welcome to the Sarbanes-Oxley Compliance Professionals Association (SOXCPA), the largest Association of Sarbanes-Oxley professionals in the world.

Join us. Stay current. Read our monthly newsletter with news, alerts, challenges and opportunities. Get certified and provide independent evidence that you are a Sarbanes-Oxley expert.

You can explore what we offer to our members:

1. Membership - Become a standard, premium or lifetime member.

You may visit: [https://www.sarbanes-oxley-association.com/How_to_become_member.htm](https://www.sarbanes-oxley-association.com/How_to_become_member.htm)

2. Monthly Updates - Visit the Reading Room of the SOXCPA at: [https://www.sarbanes-oxley-association.com/Reading_Room.htm](https://www.sarbanes-oxley-association.com/Reading_Room.htm)

3. Training and Certification - You may visit: [https://www.sarbanes-oxley-association.com/Distance_Learning_and_Certification.htm](https://www.sarbanes-oxley-association.com/Distance_Learning_and_Certification.htm)
   [https://www.sarbanes-oxley-association.com/CJSOXE_Distance_Learning_and_Certification.htm](https://www.sarbanes-oxley-association.com/CJSOXE_Distance_Learning_and_Certification.htm)

For instructor-led training, you may contact us. We tailor all programs to meet specific requirements.

4. Authorized Certified Trainer, Certified Sarbanes Oxley Expert Trainer (SOXCPA-ACT / CSOET) program - Become an ACT. This is an additional advantage on your resume, serving as a third-party endorsement to your knowledge and experience.

To learn more: [https://www.sarbanes-oxley-association.com/SOXCPA_Authorized_Certified_Trainer.html](https://www.sarbanes-oxley-association.com/SOXCPA_Authorized_Certified_Trainer.html)