*Monday, April 20, 2020*

Top 10 risk and compliance related news stories and world events that (for better or for worse) shaped the week's agenda, and what is next

Dear members and friends,

Computer Security Incident Response Teams (CSIRTs), Law Enforcement (LE) and the judiciary (prosecutors and judges) have different approaches or mindsets, as they often have different educational and scientific backgrounds.

In particular, CSIRTs have a 'technical mentality' while the judiciary has a 'legal mentality'. The LE have partly a 'legal mentality' and partly a 'technical mentality' that is entrenched in how society operates in the area of crime.

The different mentalities make communication among these three entities not always easy. This can also lead to limitations of cooperation or at least a slowdown in cooperation.

This is part of an interesting paper, *Roadmap on the cooperation between CSIRTS and LE,* from the European Union Agency for Cybersecurity (ENISA).

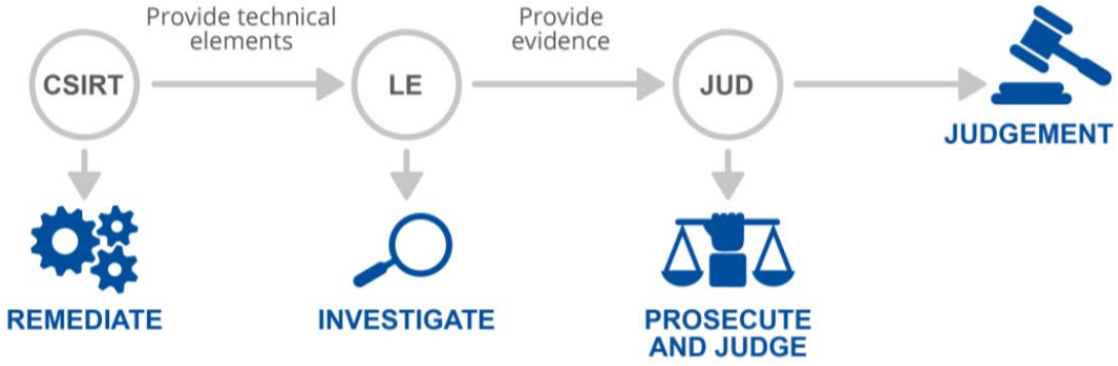
According to the paper, each community has its own discreet set of responsibilities, duties, expertise, powers and technical and procedural tools.

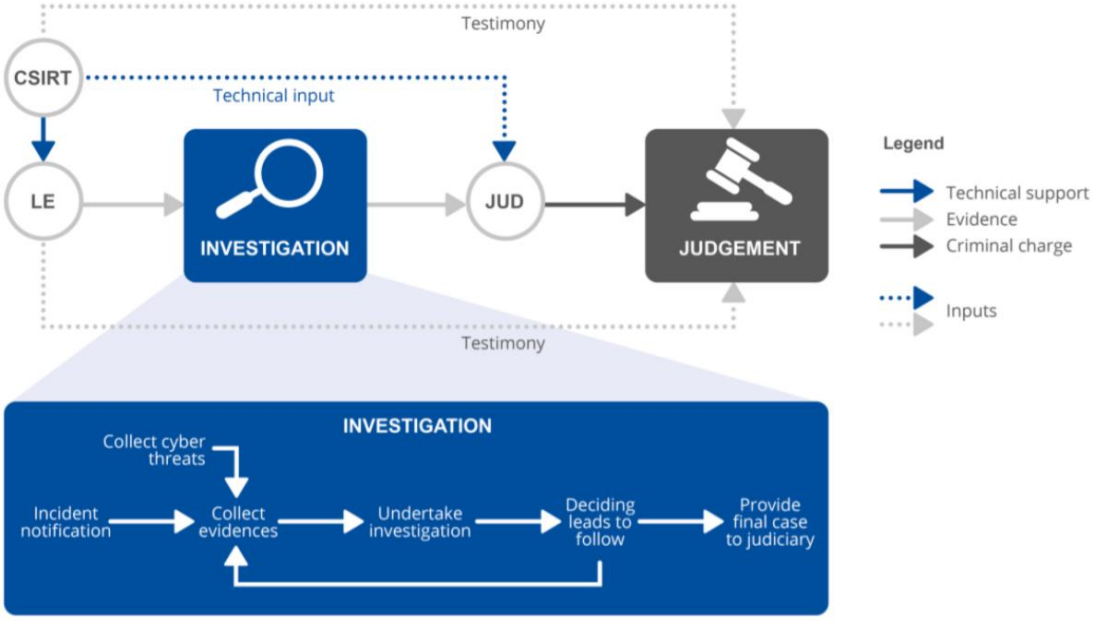
Sometimes, however, duties and responsibilities overlap, and this might lead to undesirable interference to each other's activities. Therefore, it is important for the communities to understand each other's duties.

*CSIRTs* are responsible to ensure the confidentiality, availability and integrity of systems within their constituency. *LE* aims to trace offenders

and gather evidence that describes the course of the offence and show offenders' guilt. On the basis of the results of the work of the law enforcement authorities, the *judiciary* assesses the factual and legal conclusions resulting from the evidence obtained and decides on guilt and punishment.

The CSIRTs' role is to prevent incidents from happening by implementing appropriate security measures or suggesting such measures to their constituency. And in the event of an incident, their aim is to detect and analyse the incident and apply appropriate measures, remedy the damage and subsequently secure the exploited vulnerabilities, or other existing threats.




As first responders, however, they could be also responsible for advising their constituency to report the incident to LE (or in some cases they might have themselves a duty to report), expected to share the information with other sectors or targeted industries, and required to provide necessary

assistance to other communities and collect evidence.

LE is dedicated to investigate cybercrimes and investigate possible culprits. They have legal power to mandate entities to cooperate in the investigation and disclose information or to contribute to the investigation in different ways: seizes, searches, and interceptions.

LE responsibility is to collect evidence in a lawful way, even if it may challenge remediation or business continuity. Of course, they seek to avoid further consequences to the victims, but sometimes, evidence collection can postpone remediation or return to normal.

Read more at number 3 below. Welcome to the Top 10 list.

*Best regards,*

George Lekatis
President of the IARCP
1200 G Street NW Suite 800,
Washington DC 20005, USA
Tel: (202) 449-9750
Email: lekatis@risk-compliance-association.com
Web: www.risk-compliance-association.com
HQ: 1220 N. Market Street Suite 804,
Wilmington DE 19801, USA
Tel: (302) 342-8828

*Number 1 (Page 6)*

2019 Annual Report

PCAOB
Public Company Accounting Oversight Board

*Number 2 (Page 9)*

EIOPA urges (re)insurers to temporarily suspend all discretionary dividend distributions and share buy backs

eiopa
EUROPEAN INSURANCE AND OCCUPATIONAL PENSIONS AUTHORITY

*Number 3 (Page 10)*

Supporting the fight against cybercrime

The map to the road less traveled: CSIRTs & Law Enforcement cooperation

enisa
European Network and Information Security Agency

*Number 4 (Page 13)*

Federal agencies encourage mortgage servicers to work with struggling homeowners affected by COVID-19

*Number 5 (Page 15)*

SEC Coronavirus (COVID-19) Response

*Number 6 (Page 17)*

## Statement on the Importance of High-Quality Financial Reporting in Light of the Significant Impacts of COVID-19

Sagar Teotia, Chief Accountant

*Number 7 (Page 19)*

## See how your community is moving around differently due to COVID-19

Google

*Number 8 (Page 20)*

## Civilians 'Defending Forward' in Cyberspace

Dr. Matthew J. Flynn

THE CYBER DEFENSE REVIEW

*Number 9 (Page 22)*

## Proliferated Commercial Satellite Constellations, Implications for National Security

By Matthew A. Hallex and Travis S. Cottom

JFQ | Joint Force Quarterly
Issue 97, 2nd Quarter 2020

*Number 10 (Page 24)*

## Acting Dir. Highnam Discusses COVID-19

DARPA is seizing opportunities to transition technology to support frontline defenders

DARPA DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

*Number 1*

2019 Annual Report

PCAOB

Public Company Accounting Oversight Board

*Message from the Chairman.*

The PCAOB's 2019 annual report summarizes our operations and financial results from fiscal year 2019.

It details key initiatives pursued by the Board and our dedicated staff in support of our five strategic goals during the past year.

Following the extensive strategic planning, outreach, and organizational assessment we conducted in 2018, we focused much of 2019 on advancing the changes necessary to support these goals and moving the PCAOB along the organizational maturity curve.

We took substantial steps in 2019 towards implementing our vision to transform the PCAOB into a trusted leader that promotes high quality auditing through forward-looking, responsive, and innovative oversight.

Specifically, we

(1) made changes to improve the effectiveness of our oversight activities,
(2) expanded our stakeholder outreach and improved our communications,
(3) made a number of additions and enhancements to our operations, and
(4) took steps towards optimizing our culture.

When we adopted our strategic plan in 2018 based on extensive external and internal feedback, we understood it would take several years to accomplish our goals.

That remains true today, which is why the Board collectively reaffirmed our commitment to our five-year strategic vision, values, and goals in 2019.

We are encouraged by the positive feedback we are receiving from our stakeholders on our strategic direction and the advancements made to date, particularly as it relates to the usefulness of our information and the enhanced engagement by the Board and staff.

We have made significant progress, and we remain committed to continuing that progress during 2020.

As the PCAOB's Chairman, I look forward to continuing to work collaboratively with my fellow Board Members, the U.S. Securities and Exchange Commission, and the PCAOB staff to fulfill our statutory mandate.

Respectfully

**William D. Duhnke III**
Chairman
Public Company Accounting Oversight Board

## PCAOB BY THE NUMBERS

**1,796** PCAOB-registered public accounting firms

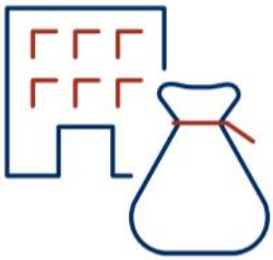
**91** Jurisdictions across the globe with PCAOB-registered public accounting firms

**597** PCAOB-registered firms audit

**12,828** issuers that file financial statements with the SEC or otherwise play a substantial role in those audits

**416** PCAOB-registered firms audit

**3,596** SEC-registered broker-dealers



**7,339** U.S. public companies, representing approximately

**$45.533** trillion in global market capitalization


The report:
https://pcaobus.org/About/Administration/Documents/Annual%20Reports/2019-PCAOB-Annual-Report.pdf

*Number 2*

## EIOPA urges (re)insurers to temporarily suspend all discretionary dividend distributions and share buy backs

The European Insurance and Occupational Pensions Authority (EIOPA) has published a statement on dividends distribution and variable remuneration policies in the context of COVID-19.

Taking due account of the current level of uncertainty on the depth, magnitude and duration of the impacts of COVID-19 in financial markets and on the economy, EIOPA urges (re)insurers to temporarily suspend all discretionary dividend distributions and share buy backs aimed at remunerating shareholders.

This suspension should be reviewed as the financial and economic impact of the COVID-19 starts to become clearer.

This prudent approach should also be applicable to the variable remuneration policies.

The statement builds on EIOPA's statement of 17 March which stressed the importance of insurers preserving their capital position in balance with the protection of the insured, following prudent dividend and other distribution policies, including variable remuneration.

The statement represents one of a series of measures that EIOPA is recommending, in close cooperation with national supervisory authorities, to mitigate the impact of the Coronavirus/COVID-19 outbreak on the insurance sector, policyholders and beneficiaries.

To read more:
https://www.eiopa.europa.eu/sites/default/files/publications/statement-on-dividend-distribution-april2020.pdf

*Number 3*

## Supporting the fight against cybercrime

The map to the road less traveled: CSIRTs & Law Enforcement cooperation

In an effort to further enhance the cooperation between the Computer Security Incident Response Teams (CSIRTs), especially national and governmental, and law enforcement agencies (LEAs), ENISA has carried out a survey and analysis of significant issues at hand that are likely to inhibit cooperation.

As ENISA usually takes a holistic view of the policy area of CSIRT and LEA cooperation, interactions with the judiciary have also been taken into consideration to the extent possible.

The result of this study is a Roadmap on the cooperation between CSIRTS and LE.

The fight against cybercrime requires the involvement of Law Enforcement Agencies (LEAs), which supported by CSIRTs are likely to be better positioned to investigate complex criminal structures.

This picture is incomplete though, unless interactions with the judiciary are equally taken into account due to the pre-eminent role it plays across the Member States in terms of directing criminal investigations.

When CSIRTs, LEAs and the judiciary cooperate, they face challenges that previously, have been categorized, by ENISA as being technical, legal, organizational and/or human behaviour as they associate with organisational culture.

Understanding these challenges is essential in an effort to tackle them, further enhance the cooperation and thus stand a better chance in the fight against cybercrime.

In 2018, ENISA confirmed that CSIRTs, LEAs and the judiciary have complementary roles and that incident handling varies across Member States. The data CSIRTs and LEAs have access to varies, and it affects information sharing between them when they seek to respond to cybercrime.

While CSIRTs interact frequently with LEAs rather than with public prosecutors, CSIRTs when collecting and analysing different types of evidence, they are called upon rarely as witness in court, even though material they collect during the incident handling typically supports an investigation and prosecution of a crime.

The data supporting this roadmap was collected via desk research, interviews with subject-matter experts and an online survey. The data collected has demonstrated that CSIRTs, LEAs and the Judiciary come across a range of challenges that are likely to impact their ability to cooperate effectively.

The legal framework has been quoted as an impeding factor when seeking to exchange data. Discrepancies in the levels of technical or legal knowledge is another one, as it may make communication challenging.

The chain of custody in evidence collection might also be an issue when using methods that might make evidence likely inadmissible in Court. Incident notifications and cybercrime reporting differ across Member States as different legal obligations might have been laid out by national law.

*Recommendations:*

- Core areas of further analysis and ENISA recommendations in an effort to improve cooperation between CSIRTs, LEAs and their interaction with the judiciary include:

- Promoting the use of 'Segregation of duties' matrix for avoiding conflicting roles and responsibilities of CSIRTs, LE and the judiciary throughout the cybercrime investigation lifecycle.

- Developing a competency framework for cybersecurity workforce and education and training policies.

- Promoting knowledge of digital forensics rules.

- Promoting interoperability of cooperation tools deployed and conceived considering future technologies.

- Assessing the suitability of cybersecurity certification for common tools and procedures.

- Simplifying arrangements by creating internal cooperation procedures to streamline exchanges.

The target audience of this roadmap includes mainly, but it is not limited to CSIRTs, LEAs, prosecutors, and judges. This roadmap builds on past ENISA work and it contributes to the implementation of the ENISA programming document 2019-2021, Output O.4.2.2.

To read more:
https://www.enisa.europa.eu/publications/support-the-fight-against-cybercrime-roadmap-on-csirt-le-cooperation

*Number 4*

## Federal agencies encourage mortgage servicers to work with struggling homeowners affected by COVID-19

Board of Governors of the Federal Reserve System
Conference of State Bank Supervisors
Consumer Financial Protection Bureau
Federal Deposit Insurance Corporation
National Credit Union Administration
Office of the Comptroller of the Currency

The federal financial institution regulatory agencies and the state financial regulators issued a joint policy statement providing needed regulatory flexibility to enable mortgage servicers to work with struggling consumers affected by the Coronavirus Disease (referred to as COVID-19) emergency.

The actions announced today by the agencies inform servicers of the agencies' flexible supervisory and enforcement approach during the COVID-19 pandemic regarding certain communications to consumers required by the mortgage servicing rules.

The policy statement and guidance issued today will facilitate mortgage servicers' ability to place consumers in short-term payment forbearance programs such as the one established by the Coronavirus Aid, Relief, and Economic Security Act (CARES Act).

Under the CARES Act, borrowers in a federally backed mortgage loan experiencing a financial hardship due, directly or indirectly, to the COVID-19 pandemic, may request forbearance by making a request to their mortgage servicer and affirming that they are experiencing a financial hardship during the COVID–19 pandemic.

In response, servicers must provide a CARES Act forbearance, that allows borrowers to defer their mortgage payments for up to 180-days and possibly longer.

The policy statement clarifies that the agencies do not intend to take supervisory or enforcement action against mortgage servicers for delays in sending certain early intervention and loss mitigation notices and taking certain actions relating to loss mitigation set out in the mortgage servicing rules, provided that servicers are making good faith efforts to provide these notices and take these actions within a reasonable time.

To further enable short-term payment forbearance programs or short-term repayment plans, mortgage servicers offering these programs or plans will not have to provide an acknowledgement notice within 5 days of receipt of an incomplete application, provided the servicer sends the acknowledgment notice before the end of the forbearance or repayment period.

The guidance also reminds servicers that there is existing flexibility in the rules with respect to the content of certain notices.

Finally, to assist servicers experiencing high call volumes from consumers seeking help, the policy statement also confirms that the agencies do not intend to take supervisory or enforcement action against mortgage servicers for delays in sending annual escrow statements, provided that servicers are making good faith efforts to provide these statements within a reasonable time.

To read more:
https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20200403a1.pdf

*Number 5*

## SEC Coronavirus (COVID-19) Response

The U.S. Securities and Exchange Commission's efforts are centered, first and foremost, on the health and safety of our employees and all Americans.

[+] Agency Operations: Transition to Telework and Continuity of Operations

[+] Market Monitoring and Engagement with Market Participants

[+] Guidance and Targeted Regulatory Assistance and Relief

[+] Enforcement, Examinations and Investor Education

[+] Effect on Comment Periods for Certain Pending Actions

We also are focused on, among other things:

- maintaining the continuity of Commission operations;
- monitoring market functions and system risks;
- providing prompt, targeted regulatory relief and guidance to issuers, investment advisers and other registrants impacted by COVID-19 to facilitate continuing operations, including in connection with the execution of their business continuity plans (BCPs); and
- maintaining our enforcement and investor protection efforts, particularly with regard to the protection of our critical market systems and our most vulnerable investors.

We continue to work in close coordination with other financial regulators and governmental authorities in the United States and globally.

Through this period of collective, national challenge, we have remained fully operational and committed to our tripartite mission to protect investors; maintain fair, orderly, and efficient markets; and facilitate capital formation.

While the agency is engaging on numerous COVID-19 initiatives as noted above, we also continue our regular agency operations.

For example, we have continued to advance rulemaking initiatives, conduct risk-based inspections, bring enforcement actions, and review and comment on issuer and fund filings.

Our staff has been intently focused on continuing to display the level of professionalism and dedication on which our investors and markets have come to rely.

We recognize the importance of our mission to America's investors and our markets and believe it is a privilege to serve.

To read more: https://www.sec.gov/sec-coronavirus-covid-19-response

*Number 6*

## Statement on the Importance of High-Quality Financial Reporting in Light of the Significant Impacts of COVID-19

Sagar Teotia, Chief Accountant

## Introduction

The Office of the Chief Accountant (OCA), along with the Commission and other Divisions and Offices of the SEC, is closely monitoring the impact of issues raised by coronavirus disease 2019 (COVID-19) on investors and global capital markets.

As Chairman Clayton said in his recent statement, we are facing an unprecedented national challenge – a challenge that has significant implications for financial reporting, our markets, and our economy more generally.

As we face these challenging times, investors and other stakeholders need high-quality financial information more than ever.

The proper functioning of our capital markets depends on a regular supply of high-quality financial information that enables investors, lenders, and other stakeholders to make informed decisions.

Although markets and companies face uncertainties, we have a robust and longstanding financial reporting system in place, including the accounting, disclosure, and auditing models that will help us to address recent challenges.

Where appropriate, the Commission and the staff have been ready to assist market participants with financial reporting issues.

For example, the Commission recently issued an order conditionally extending the temporary 45-day grace period for registrants affected by COVID-19 to file Exchange Act reports to include reports due through July 1, 2020.

The Division of Corporation Finance also provided guidance for companies as they assess COVID-19-related effects and consider their disclosure obligations.

OCA continues to focus on investors' need for high-quality financial information, and on our mission and priorities as described in our Statement in Connection with the 2019 AICPA Conference on Current SEC and PCAOB Developments.

Importantly, to further high-quality financial information, we are available to help companies, auditors, and others with complex accounting, financial reporting, independence, and auditing issues.

We are taking a proactive approach and have been engaged with stakeholders across the financial reporting ecosystem – e.g., preparers, auditors, audit committee members, investors, standard setters, and other regulators – on issues related to current market developments.

We remain available for consultation and encourage stakeholders to contact our office with questions they encounter as a result of COVID-19.

The following paragraphs address some of OCA's work and how we have been responding to COVID-19. We expect that our work in this area will be ongoing for the foreseeable future.

To read more:
https://www.sec.gov/news/public-statement/statement-teotia-financial-reporting-covid-19-2020-04-03

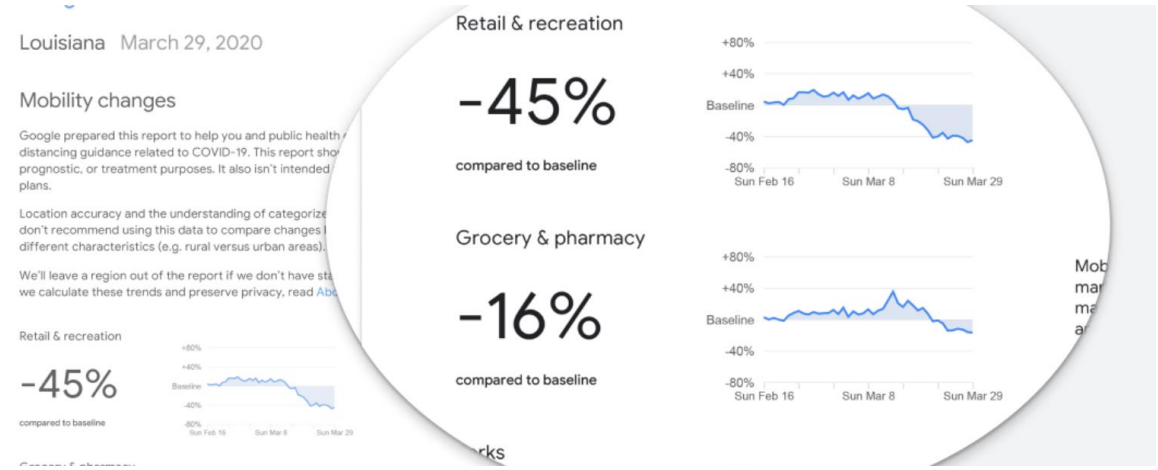
*Number 7*

## See how your community is moving around differently due to COVID-19

As global communities respond to COVID-19, we've heard from public health officials that the same type of aggregated, anonymized insights we use in products such as Google Maps could be helpful as they make critical decisions to combat COVID-19.

These Community Mobility Reports aim to provide insights into what has changed in response to policies aimed at combating COVID-19.

The reports chart movement trends over time by geography, across different categories of places such as retail and recreation, groceries and pharmacies, parks, transit stations, workplaces, and residential.




You may visit:
https://www.google.com/covid19/mobility/

*Number 8*

## Civilians 'Defending Forward' in Cyberspace

Dr. Matthew J. Flynn

THE CYBER DEFENSE REVIEW

Examining the 'defending forward' concept and the intersection between DoD and the private sector speaks to aligning instruments of national power to set the stage for the consolidation of Internet connectivity and an expansion of that capability.

Both outcomes feed a new understanding of what a professional military does in the cyber age to safeguard a civilian interface that is revamping the norms of government across state boundaries.

Implementing an effective cyber strategy necessitates recasting the US military's cyber operations to support civilian efforts.

A dramatic point of departure from the current emphasis, this change in focus will prevent the US military from leading a non-violent conflict at odds with war in the corporal world.

Instead, civilians will be charged with winning the fight in the cognitive arena of cyberspace.

Civilian entities have put themselves in a state of readiness in terms of cyber security that begs the question of exactly what role the US military should play in cyberspace.

In several ways, private business is 'defending forward' and waging war in cyberspace, overtly at times.

This effort means that the civilian sector seeks to disrupt and halt malicious cyber activity at its source, and degrades such activity before it can reach its intended victims, in parallel with the aim of the Department of Defense's (DoD) new mandate of defending forward.

Detecting and reporting threats from malicious online actors, revealing how those actors frequently work at the behest of nation states, and offering exploits to counter such activity are essential elements of the DoD's active preparedness in cyberspace.
This positioning also means an attempt to exceed the defense of critical resources and related sectors of the economy to engage in a messaging war that accompanies technical attacks and threats in cyberspace.

Yet, the private sector already engages in an online information offensive, and in so doing counters the potential of an inimical US military presence in cyberspace looking to police thoughts exchanged on the Internet.

Recognition of the private sector's needed ability to check military largess in this capacity is only slowly coming into focus, but may well constitute the most important measure of the defending forward strategy.

This article calls for the US military to accept the civilian defense of an open Internet that is critical to the success of the future of cyberspace.

Leveraging the status quo of "openness" centers attention on the Clausewitzian contest of wills in order to pursue a change in mindset more than a correction in behavior assumed to accompany an act of military force.

Defending forward in cyberspace with civilians in the lead can achieve a lasting impact via an act of coercion that seeks a cognitive end, less a physical measure.

That intellectual application of war, the most essential measure of a contest of wills, is well-suited to the ether of cyberspace.

In providing a service facilitating a population's access to the Internet and doing so without government oversight, the private sector has delivered the most important function of openness.

Whether by balloons, drones, or satellites, these companies provide connectivity to some three billion people and now look to connect the rest of humanity, a further five billion people.

This goal may prove overly ambitious, but it means that the number of people online will continue to rise.

Even assigning the self-interested motive of gaining market share to those businesses so engaged does little to forestall the reality that with more people online, connectivity remains a powerful reality and so too openness.

To read more (page 31/204):
https://cyberdefensereview.army.mil/Portals/6/CDR%20V5N1%20-%20FULL_WEB_1.pdf

*Number 9*

## Proliferated Commercial Satellite Constellations, Implications for National Security

By Matthew A. Hallex and Travis S. Cottom

JFQ | Joint Force Quarterly
Issue 97, 2nd Quarter 2020
National Defense University Press
The premier professional military and academic publishing house

The falling costs of space launch and the increasing capabilities of small satellites have enabled the emergence of radically new space architectures—proliferated constellations made up of dozens, hundreds, or even thousands of satellites in low orbits.

Commercial space actors—from tiny startups to companies backed by billions of dollars of private investment— are pursuing these new architectures to disrupt traditional business models for commercial Earth observation and satellite communications.

The success of these endeavors will result in new space-based services, including global broadband Internet coverage broadcast from orbit and high-revisit overhead imagery of much of the Earth's surface.

The effects of proliferated constellations will not be confined to the commercial sector.

The exponential increase in the number of satellites on orbit will shape the future military operating environment in space.

The increase in the availability of satellite imagery and communications bandwidth on the open market will also affect the operating environment in the ground, maritime, and air domains, offering new capabilities that can address hard problems facing the U.S. military, such as tracking mobile targets, operating in the Arctic, or providing resilient space support in the face of growing counterspace threats.

These trends will also create new challenges as adversaries ranging from Great Power competitors to hostile nonstate actors gain cheap access to space capabilities and the emergence of space-based Internet reshapes the cyber battlespace.

This article discusses some of the proposed commercial proliferated constellations being developed in the United States and abroad and

explores the potential effects of proliferated constellations on the space, terrestrial, and cyber domains.

It identifies the multidomain challenges and opportunities these trends create for the warfighter and proposes steps that the Department of Defense (DOD) and the broader national security community can take to prepare.

To read more (page 23/132):
https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-97/jfq-97.pdf

*Number 10*

## Acting Dir. Highnam Discusses COVID-19

DARPA is seizing opportunities to transition technology to support frontline defenders

DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

The United States confronts a potential national security threat each time a new outbreak of infectious disease occurs anywhere in the world. Our military must be able to deploy safely to wherever they are required to operate.

The disease threats seen abroad can also impact the civilian population. The nationwide spread of H1N1 flu in 2009, of Middle East Respiratory Syndrome in Indiana in 2013, and the presence of Ebola in Texas in 2014 are recent reminders of this reality.

As the current COVID-19 pandemic shows, an unwarned highly contagious virus can rapidly overwhelm medical systems worldwide.

There is currently a mismatch between the rapidity at which biological threats can emerge and proliferate and the response time for developing and deploying effective medical countermeasures.

Traditional biodefense technologies are primarily to counter known pathogens, and even then, long lead times may be required to develop responses.

After creating a successful medical countermeasure, it must then be mass-produced and stockpiled in preparation for a large-scale emergency.

This process is time-consuming enough for known and predictable threats. It can be agonizingly slow when it comes to unfamiliar pathogens like SARS-CoV-2 (the cause of the COVID-19 illness), which can spread at pandemic scale before scientists can devise and deploy countermeasures.

Cognizant of the need for speed, DARPA began aggressively pursuing medical countermeasures research more than a decade ago with a focus on developing generalizable, virus-agnostic technologies that can address whatever threat emerges, rather than building a collection of one-off solutions.

This approach allows “firebreaks” to mitigate the national security risks posed by infectious disease, and is illustrative of a portfolio of biological programs aimed at preventing pandemics.

During this uncertain time, we would like to stress that we are working on several fronts to bring the latest science and technology to overtake the challenges posed by COVID-19.

The agency’s primary concern, of course, is for the health and safety of its personnel, partners, performers, as well as the broader defense and research community it supports.

The agency is monitoring the COVID-19 situation and is appropriately adjusting its work policies for its employees and contractors based on public health guidelines and the policies put in place by federal, state, and local officials.

We are not naïve to the realities of our current operating environment and know there will be challenges ahead as remote work, facility closures, and other restrictions are put in place to keep people safe.

We are working with those impacted to strike an appropriate balance between operating safely while continuing to pursue our critical research for national defense.

That said, over these next few months we will undoubtedly see impacts on the progress made across our research programs as well as our ability to transition technologies.

We continue to push forward on our mission and are confident that, despite the challenges, DARPA will deliver breakthrough technologies during and after this difficult time.

As you would expect, DARPA is identifying and seizing opportunities to accelerate research and technology transitions to support our frontline defenders in the military and in medical facilities nationwide.

Going forward, we intend to use this space to update you on the latest news regarding DARPA’s programs dedicated to preventing pandemics.

All of us have a role to play in ensuring that DARPA succeeds in its mission; and we hope you stay engaged with and inspired by our actions in the difficult days ahead.

Yours,

Peter Highnam, Ph.D.
Acting Director
Defense Advanced Research Project Agency

## 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 individual or entity;

- should not be relied on in the 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 regarding such problems incurred because of using this site or any linked external sites.

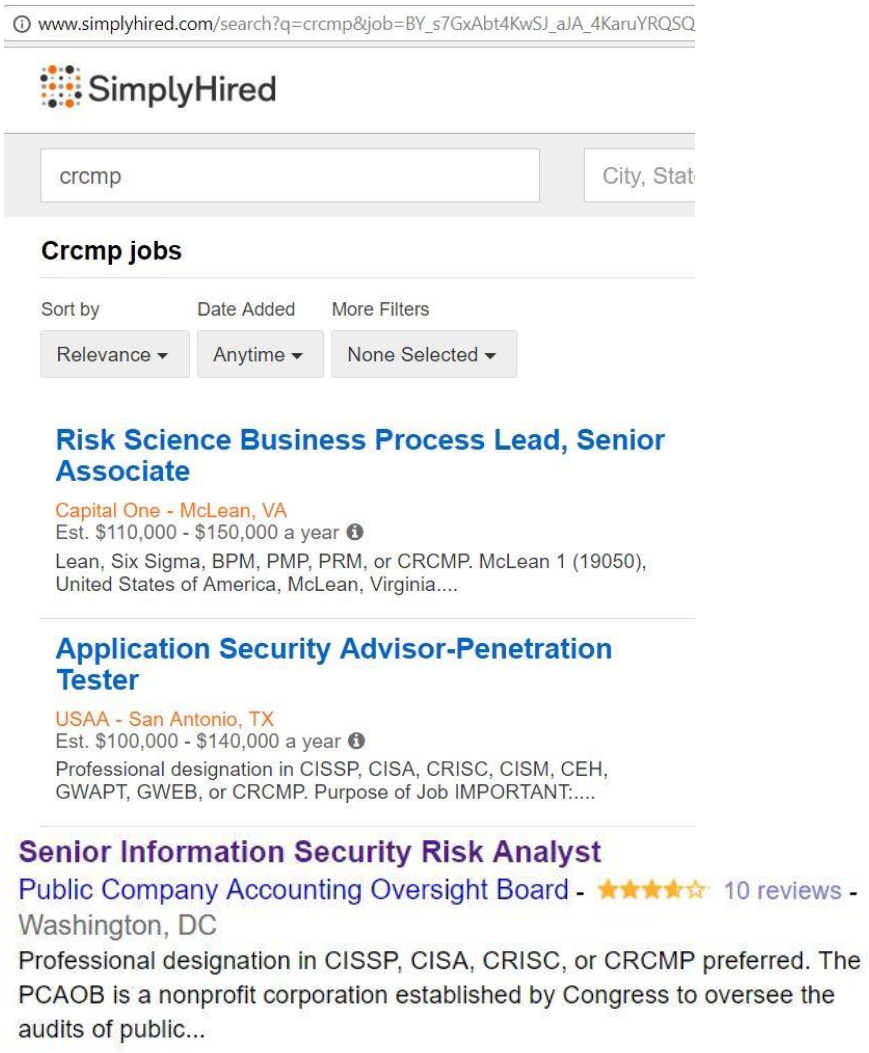
# International Association of Risk and Compliance Professionals

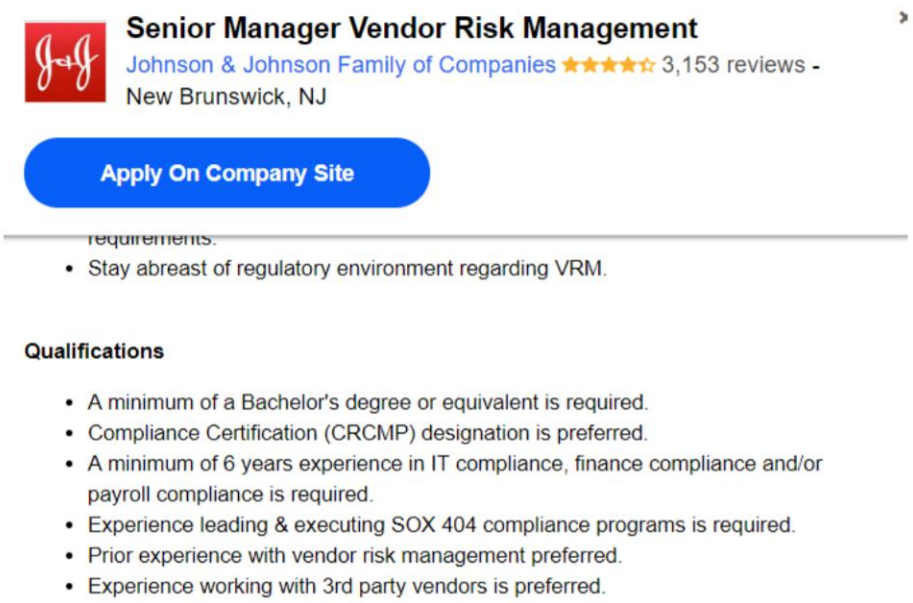
You can explore what we offer to our members:

1. *Membership* – Become a standard, premium or lifetime member.
You may visit:
https://www.risk-compliance-association.com/How_to_become_member.htm

2. *Weekly Updates* - Visit the *Reading Room* of the association at:
https://www.risk-compliance-association.com/Reading_Room.htm

3. *Training and Certification* – Become a Certified Risk and Compliance Management Professional (CRCMP), a Certified Information Systems Risk and Compliance Professional (CISRCP), a Certified Cyber (Governance Risk and Compliance) Professional - CC(GRC)P, and / or a Certified Risk and Compliance Management Professional in Insurance and Reinsurance - CRCMP(Re)I.





**Senior Manager Vendor Risk Management**

Johnson & Johnson Family of Companies ★★★★☆ 3,153 reviews -
New Brunswick, NJ

Apply On Company Site

requirements.

- Stay abreast of regulatory environment regarding VRM.

**Qualifications**

- A minimum of a Bachelor's degree or equivalent is required.
- Compliance Certification (CRCMP) designation is preferred.
- A minimum of 6 years experience in IT compliance, finance compliance and/or payroll compliance is required.
- Experience leading & executing SOX 404 compliance programs is required.
- Prior experience with vendor risk management preferred.
- Experience working with 3rd party vendors is preferred.

Companies and organizations like Accenture, American Express, USAA etc. consider the Certified Risk and Compliance Management Professional (CRCMP) program a preferred certificate. There are CRCMPs in 32 countries.

You can find more about the demand for CRCMPs at:
https://www.risk-compliance-association.com/CRCMP_Jobs_Careers.pdf

For the Certified Risk and Compliance Management Professional (CRCMP) distance learning and online certification program, you may visit:
https://www.risk-compliance-association.com/Distance_Learning_and_Certification.htm

For the Certified Information Systems Risk and Compliance Professional (CISRCP) distance learning and online certification program, you may visit:
https://www.risk-compliance-association.com/CISRCP_Distance_Learning_and_Certification.htm

For the Certified Cyber (Governance Risk and Compliance) Professional - CC(GRC)P distance learning and online certification program, you may visit:
https://www.risk-compliance-association.com/CC_GRC_P_Distance_Learning_and_Certification.htm

For the Certified Risk and Compliance Management Professional in Insurance and Reinsurance - CRCMP(Re)I distance learning and online certification program, you may visit:
https://www.risk-compliance-association.com/CRCMP_Re_I.htm

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

4. *IARCP Authorized Certified Trainer (IARCP-ACT) Program* - This is an additional advantage on your resume, serving as a third-party endorsement to your knowledge and experience.


Certificates are important when being considered for a promotion or other career opportunities. You give the necessary assurance that you have the knowledge and skills to accept more responsibility.

To learn more, you may visit:
https://www.risk-compliance-association.com/IARCP_ACT.html

5. *Approved Training and Certification Centers (IARCP-ATCCs)* - In response to the increasing demand for CRCMP training, the International Association of Risk and Compliance Professionals is developing a world-wide network of Approved Training and Certification Centers (IARCP-ATCCs).


This will give the opportunity to risk and compliance managers, officers, and consultants to have access to instructor led training at convenient locations that meet international standards.

ATCCs use IARCP approved course materials and have access to IARCP Authorized Certified Trainers (IARCP-ACTs).

To learn more:
https://www.risk-compliance-association.com/Approved_Centers.html