Monday, February 17, 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,

I have just read for the second time the report from the US Office of Intelligence & Analysis with title *Strategic Plan for Fiscal Years 2020-2024*. The Office of Intelligence & Analysis is the first federal agency statutorily mandated to share intelligence with state, local, tribal, and territorial law enforcement, as well as the private sector.

We read: "Emerging disruptive technologies continue to outpace legislation and countermeasures across the Homeland.

Unmanned aerial systems (UAS) will continuously enable transnational criminal organizations and criminals to carry out cross-border drug smuggling operations.

Actors will continue to use UAS to conduct surveillance of law enforcement, and potentially facilitate kinetic attacks on stationary, mobile, and high-consequence targets.

Additionally, nefarious actors are increasingly acquiring new capabilities, and enhancing their use of technology previously only accessible to nation-state actors."

I remember a 1970 book, written by Alvin Toffler, with title *Future Shock*. According to Alvin, "It is undeniably true that we frequently apply new technology stupidly and selfishly. In our haste to milk technology for immediate economic advantage, we have turned our environment into a physical and social tinderbox. Our technological powers increase, but the side effects and potential hazards also escalate."

We can see that it is not the first time we are concerned about emerging disruptive technologies. But as we can see in the recent I&A Strategic Plan 2020-2024, during this era of dynamic threats that cross borders in both the physical and digital arenas, we need more and more intelligence and information on transnational organized crime, terrorism, cyber-threat actors, counterintelligence vulnerabilities, economic security, and other developing threats that pose a critical danger to security and the democratic way of life.

Read more at number 8 below. Welcome to the Top 10 list.

Best regards,

George Lekatis

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 5)

Stress testing in Latin America: A comparison of approaches and methodologies

BIS Papers, No 108. Report submitted by a study group established by the BIS CCA Consultative Group of Directors of Financial Stability (CGDFS) and chaired by Pamela Cardozo, Bank of the Republic, Colombia. Monetary and Economic Department, February 2020.

Number 2 (Page 8)

2019 Annual report

Number 3 (Page 11)

EBA consults on revised guidelines on money laundering and terrorist financing risk factors

Number 4 (Page 13)

Running on Empty: A Proposal to Fill the Gap Between Regulation and Decentralization

Commissioner Hester Peirce, Chicago, IL.

Number 5 (Page 26)

Election security

DHS Plans Are Urgently Needed to Address Identified Challenges Before the 2020 Elections

Number 6 (Page 30)

Bank funding costs and solvency

Staff Working Paper No. 853 - Guillaume Arnould, Cosimo Pancaro and Dawid Żochowski, February 2020

Number 7 (Page 33)

Guidelines on outsourcing to cloud service providers now available for national supervisory authorities

Number 8 (Page 35)

Office of Intelligence & Analysis Strategic Plan for Fiscal Years 2020-2024.

Number 9 (Page 37)

Improving 5G Network Security

Number 10 (Page 40)

Code repository used to host and distribute malware

Number 1

Stress testing in Latin America: A comparison of approaches and methodologies

BIS Papers, No 108. Report submitted by a study group established by the BIS CCA Consultative Group of Directors of Financial Stability (CGDFS) and chaired by Pamela Cardozo, Bank of the Republic, Colombia. Monetary and Economic Department, February 2020.

Since the Great Financial Crisis, bank supervisors and central banks have greatly increased and intensified their use of stress tests.

The literature on stress testing has also expanded, but it generally focuses on the practice of policymakers in advanced economies and the challenges they face.

Less is known about stress testing in emerging market economies and Latin American countries in particular.

The purpose of this report is to fill this gap.

The report is based on the information gathered by a study group on stress testing formed by the Consultative Group of Directors of Financial Stability (CGDFS) and comprising selected central banks in the Americas.

The study group held several meetings in person and through video conferences, conducted surveys and undertook a common exercise.

The common stress-testing exercise proved particularly informative.

Each participating jurisdiction ran their typical top-down stress tests under an agreed common scenario, making it easier to compare methodologies and approaches.

To the best of our knowledge, this is the first report that systematically compares the stress test methodologies of Latin American central banks.

The report finds that the main type of test run by central banks is a top-down solvency stress test.

Supervisory agencies conduct banking stress tests independently, usually of the bottom-up type.

Coordination between the central bank and the supervisory agency, usually informal, is widespread.

It takes place regularly, with the aim of facilitating the efficient exchange of information and opinions, the comparison of stress test results, and the provision of feedback on methodologies.

Central bank stress tests focus mainly on banks, including all banking system participants.

In some cases, they also include other deposit-taking institutions.

The number of entities covered, as well as the sample composition, varies greatly between jurisdictions.

Credit and market risks are the main risk categories assessed, usually over a horizon of two or three years.

Some jurisdictions also cover other risks or the strength of transmission channels using specific models distinct from the main stress test engine.

Central banks rely on supervisory bank-level data to run their stress tests, sometimes disaggregating loans by sector and using banks' income statements.

Credit risk assessment requires data on loans, charge-offs and loan loss provisions for commercial, consumer and mortgage loans at a system level as well as data on credit portfolios using broad and historic information on defaults at the bank/category levels.

The assessment of market risk usually requires individual bank information, such as detailed portfolio holdings by institution, and financial market data such as interest rate curves and exchange rates.

Assessing the strength of contagion requires detailed information on interbank exposure.

The frequency of the data used in the stress tests usually depends on their availability.

As baseline scenarios, central banks typically use market surveys or projections produced by other central bank departments.

The design of the stressed scenarios involves specifying the magnitude, direction and dynamics of the shocks to the key macroeconomic variables.

The methodologies used include multivariate econometric models, replication of historical events or statistical rules applied to some or all variables in the scenario.

In addition, central banks commonly use expert judgment, and in some cases, also the financial and macroeconomic risks identified by private sector.

To read more: https://www.bis.org/publ/bppdf/bispap108.pdf

Objectives of top-down stress testing — Table 1

	Argentina	Brazil[3]	Chile[4]	Colombia	Mexico	Peru	Uruguay
Surveillance (macroprudential)[1]							
Solvency							
Authorities' own assumptions, by individual bank		•		•	•		•
Authorities' own assumptions, by group of banks		•				•	
Authorities' own assumptions, system-wide		•	•			•	•
Liquidity							
Authorities' own assumptions, by individual bank		•	•	•			•
Authorities' own assumptions, by group of banks							
Authorities' own assumptions, system-wide		•					•
Supervisory (microprudential)[2]							
Solvency	•	•				•	•
Liquidity	•	•					•

Number 2

2019 Annual report

The U.S. economy has continued to perform well since the publication of the previous report of the Council in December 2018.

Contents

Economic growth remains robust, unemployment rates are at a fifty year low, corporate and consumer delinquency and default rates are low, and financial conditions are broadly stable.

Stock prices have increased over the past year. Prices for commercial and residential real estate have also increased albeit at a somewhat slower rate than in previous years.

However, some uncertainty regarding future economic performance has emerged. This uncertainty prompted the Federal Reserve to shift to a more accommodative monetary policy stance over the past year.

Overall, risks to U.S. financial stability remain moderate. Much of the uncertainty in the economic outlook stems from events overseas.

A slowdown in economic growth in the euro area and China may affect economic conditions in the United States though the effects on financial stability, if any, are likely to be modest.

The potential for a disorderly withdrawal of the United Kingdom from the European Union (EU) remains.

Such an event could impact global markets and have a further negative impact on European economic growth.

Domestically, the growth in corporate borrowing remains a key area of focus for the Council.

While firms are able to service their obligations in the current economic environment, high levels of debt and leverage in the corporate sector could exacerbate the effects of a sharp reversal in economic conditions. Maintaining a resilient financial system is important.

The economic well-being of Americans depends on the ability of the financial system to provide capital to businesses and individuals, to provide vehicles for savings, and to intermediate financial transactions even in the face of adverse events.

Post-crisis regulatory reforms have strengthened the ability of the financial system to withstand a shock or an economic downturn.

However, the financial services industry and financial regulators must continue to adapt to changing circumstances.

One change in the near future is the anticipated cessation or degradation of LIBOR as a reference rate for financial contracts.

Widespread failure of market participants to adequately adapt could result in a reduction in liquidity in markets for several types of financial contracts and could potentially adversely impact financial stability.

The Council is closely monitoring developments in this area and remains vigilant regarding other potential emerging threats to financial stability.

The report:
https://home.treasury.gov/system/files/261/FSOC2019AnnualReport.pdf


E PLURIBUS
FSOC
FINANCIAL STABILITY OVERSIGHT COUNCIL

Number 3

EBA consults on revised guidelines on money laundering and terrorist financing risk factors

The EBA has issued a public consultation on revised money laundering and terrorist financing (ML/TF) risk factors Guidelines as part of a broader communication on AML/CFT issues.

This update takes into account changes to the EU Anti Money Laundering and Counter Terrorism Financing (AML/CFT) legal framework and new ML/TF risks, including those identified by the EBA's implementation reviews.

These Guidelines are central to the EBA's work to lead, coordinate and monitor the fight against money laundering and terrorist financing, explained in the accompanying factsheet.

The consultation runs until 5 May 2020.

These Guidelines, which are addressed to both financial institutions and supervisors, set out factors that institutions should consider when assessing the ML/TF risk associated with a business relationship or occasional transaction.

In addition, they provide guidance on how financial institutions can adjust their customer due diligence measures to mitigate the ML/TF risk they have identified.

Finally, they support competent authorities' AML/CFT supervision efforts when assessing the adequacy of firms' risk assessments and AML/CFT policies and procedures.

In its revised version, the EBA is proposing key changes, including new guidance on compliance with the provisions on enhanced customer due diligence related to high-risk third countries.

New sectoral guidelines have been added on crowdfunding platforms, corporate finance, payment initiation services providers (PISPs) and account information service providers (AISPs) and for firms providing activities of currency exchanges offices.

The revised Guidelines also provide more details on terrorist financing risk factors and customer due diligence (CDD) measures including on the identification of the beneficial owner, the use of innovative solutions to identify and verify the customers' identity.

In addition, they set clear regulatory expectations of firms' business-wide and individual ML/TF risk assessments.

The proposed changes will significantly strengthen Europe's AML/CFT defences and foster greater convergence of supervisory practices in areas where supervisory effectiveness has been hampered, so far, by divergent approaches in the implementation of the same European legal requirements.

To read more:
https://eba.europa.eu/eba-consults-revised-guidelines-money-laundering-and-terrorist-financing-risk-factors

Number 4

Running on Empty: A Proposal to Fill the Gap Between Regulation and Decentralization

Commissioner Hester Peirce, Chicago, IL.

Thank you George [Chikovani] for that kind introduction. I appreciate the opportunity to be with all of you today. Before beginning, I have to remind you that the views I express are my own and do not necessarily represent those of the Securities and Exchange Commission or my fellow Commissioners.

Indeed, the views I will express today are not fully formed in my own mind and may not reflect my own opinions in the months to come. To that end, I welcome the feedback of all of you and anyone else with an interest in the regulation of digital assets.

These issues are difficult, and many bright minds on the Commission's staff and outside are trying hard to develop a reasonable framework. As I thought about talking with you today, a story—one that predates my career as a regulator, but nevertheless informs it—bubbled out of my memory.

More than two decades ago, I was on a road trip. I was lost. I did not have a cell phone. It was very late at night. It was pouring. The gas gauge was on empty. There was no gas station in sight. I was distraught until two things happened.

First, I saw the lights of a lone gas station blinking in the not-too-far distance.

Second, I realized that I was in New Jersey! Recalling something a college friend had told me, I would not have wanted to be anywhere else on a stormy night with an empty gas tank.

This friend, who had grown up in New Jersey, had never pumped gas in her life—a deficiency she attributed to a New Jersey law that allowed only gas station employees to pump gas. Everybody else was prohibited from pumping gas.

That law sounded a little silly at the time, but now that I was in New Jersey about to enjoy this mandated luxury on a rain-drenched night, it sounded just wonderful.

Relieved that the fumes in my tank got me to the station, I pulled up to the pump, which, incidentally, was not under a roof substantial enough for even a rain shower, let alone this downpour.

There it was—the unequivocal sign saying that it was illegal for anyone other than a gas station attendant to pump gas. I waited expectantly for the station attendant, roused from a comfortable slumber by my arrival, to emerge from his booth and start the pump.

He looked at me. I looked at him. He pointed at me. He pointed at the pump. His message was clear—forget the law, there would be no full service on that dark and stormy night.

I will not tell you what choice I made, but let's just say that the soundtrack for that drive was Bruce Springsteen's State Trooper: "New Jersey Turnpike ridin' on a wet night 'neath the refinery's glow . . . I got a clear conscience 'bout things I done. Mister state trooper, please don't stop me."

A sensible regulatory framework would have not prevented my pumping the gas rather than being stranded in the rainy dark of night. Perhaps the New Jersey law had a hardship exemption to cover just such situations, but the empty gas tank and sign prohibiting me from filling it seemed irreconcilable at the time.

In any case, the memory of that incident brought with it a basic lesson as I think about regulation of digital assets. It is important to write rules that well-intentioned people can follow.

When we see people struggling to find a way both to comply with the law and accomplish their laudable objectives, we need to ask ourselves whether the law should change to enable them to pursue their efforts in confidence that they are doing so legally.

Entrepreneurs across the crypto landscape are facing just such a scenario in their attempts to develop worthwhile and beneficial products.

Whether it is issuing tokens to be used in a network, launching an exchange-traded product based on bitcoin, providing custody for crypto assets, operating a broker-dealer that handles crypto transactions, or setting up an alternative trading system where people can trade crypto assets, our securities laws stand in the way of innovation.

While I look forward to working with people in the community to develop solutions to each of these problems, today, I am going to focus on how to address the regulatory difficulties faced by people who want to build functioning token networks.

Before detailing my proposal for a safe harbor, I will first outline the problem. Many crypto entrepreneurs are seeking to build decentralized networks in which a token serves as a means of exchange on, or provides access to a function of the network.

In the course of building out the network, they need to get the tokens into the hands of other people. But these efforts can be stymied by concerns that such efforts may fall within the ambit of federal securities laws.

The fear of running afoul of the securities laws is real. Given the SEC's enforcement activity in this area, these fears are not unfounded.

The SEC has scrutinized token sales through the lens of SEC v. Howey, a now infamous case describing what an investment contract is. An investment contract is one type of security under our federal securities laws.

The Howey case dealt with the sale of orange groves, and subsequent cases have involved the sale of a host of other esoteric assets.

In the Howey case, purchasers of units in the orange grove were deemed to be purchasing securities because they were buying the managerial efforts of others along with their piece of the orange grove.

The SEC has tried to apply the Howey analysis to crypto, but doing so is not particularly easy.

For example, some commentators have pointed out that we have elided the distinction between the token and the investment contract.

The "contract, transaction or scheme" by which the token is sold may constitute an investment contract; but, the object of the investment contract—the token—may not bear the hallmarks of a security.

Conflating the two concepts has limited secondary trading and has had disastrous consequences for the ability of token networks to become functional.
Also of concern, suggesting that tokens will increase in value, combined with securing secondary market trading, can trigger a conclusion that those tokens are being sold pursuant to an investment contract.

There are circumstances in which the security label fits, but, in other cases, promises made about tokens increasing in value are nothing more than expressions of the hope that a network will succeed and be used by lots of people.

I would argue that the analysis should focus on the objective nature of the thing offered to the purchasers.

If the token seller is simply discussing the potential for an increase in the value of a token in the same manner that a seller of any number of other consumer products might appeal to purchasers' desire to buy a product of lasting or even increasing value, it there an investment contract? The subjective intent of any particular purchaser should not be controlling.

If it were, then is there any end to the Commission's authority? How would that logic apply to a shoe company, which, as it sells you a pair of sneakers, promises to hire some prominent athletes to promote the brand, thus focusing your mind on how sky high the price will go on StockX rather than on how high your new kicks will enable you to jump on the basketball court?

The SEC's approach in these cases has made it extremely difficult for a company to distribute a token—a process that typically includes planning for a future in which people use the network and talking positively about its prospects for success—without running into a charge that the company is engaged in a securities offering.

We have even hinted that a token airdrop in which tokens are given out freely might constitute an offering of securities. How is a person supposed to get a network up and running when she cannot even give away the tokens necessary to use the network?

One option is to stay far away from the securities laws by simply releasing a white paper, publishing the open source code, mining the genesis block, and then stepping back to allow a network of users blossom organically. Other entrepreneurs, however, might choose to remain actively and publicly involved in building a network for some time.

Some of these people have chosen to proceed with their token offerings as planned in the hopes that they can avoid scrutiny under the securities laws and perhaps convince the SEC that their networks are sufficiently functional to avoid the securities label.

This approach is risky because proving that tokens have utility prior to being distributed to a widespread user base is difficult.

Another option is for the developers to sell the tokens in a registered offering or pursuant to an exemption from registration. To date, no registered offering of tokens has been conducted in the United States.

Many token offerings have proceeded under exemptions from registration, typically Regulation D exemptions that require tokens be sold exclusively to accredited investors with transfer restrictions.

Given the limited pool of persons qualifying as accredited investors based on the current wealth and income tests, it can be difficult for these projects' networks to take off.

Several issuers of tokens have opted for conducting exempt offerings pursuant to Regulation A. However, the costs of conducting one of these so-called "mini-IPOs" can be prohibitive. Even if a team has the financial resources to take this route, once the token is a security, it must trade as a security.

A core benefit of a token network is its non-reliance on intermediaries; people transact directly with one another. Having to buy or sell tokens through a registered broker-dealer or on a registered exchange certainly puts a damper on the development of a thriving, decentralized crypto network.

Particular problems arise because there are unique challenges related to broker-dealers and exchanges handling digital assets.

Other projects have sought to sever any ties with the United States to avoid the reach of our securities laws. This approach is risky because invariably some activity occurs in the United States.

Moreover, this approach is detrimental to the US economy because it prevents American citizens from participating in budding token networks. It is evident that any route chosen by a team to distribute tokens into the hands of potential users is fraught with uncertainty under the securities laws.

We have created a regulatory Catch 22. Would-be networks cannot get their tokens out into people's hands because their tokens are potentially subject to the securities laws.

However, would-be networks cannot mature into a functional or decentralized network that is not dependent upon a single person or group to carry out the essential managerial or entrepreneurial efforts unless the tokens are distributed to and freely transferable among potential users,

developers, and participants of the network. The securities laws cannot be ignored, but neither can we as securities regulators ignore the conundrum our laws create.

There is, I think, a way to address the uncertainty of the application of the securities laws to tokens.

The safe harbor I am laying out this morning recognizes the need to achieve the investor protection objectives of the securities laws, as well as the need to provide the regulatory flexibility that allows innovation to flourish.

Accordingly, the safe harbor protects token purchasers by requiring disclosures tailored to their needs, preserving the application of the antifraud provisions of the securities laws, and giving them an ability to participate in networks of interest to them.

The safe harbor also provides network entrepreneurs sufficient time to build their networks before having to measure themselves against a decentralization or functionality yardstick.

I have spoken openly about my intention to sketch out a safe harbor, and in response, I have gotten some very helpful feedback. But before detailing the specifics of my proposal, I want to emphasize that this remains a work in progress.

I look forward to additional input, and, if I am able eventually to convince my colleagues to add consideration of such an approach to the SEC rulemaking agenda, many other voices, I hope, will weigh in.

For now, the text of the proposed safe harbor is available for viewing as an appendix to this speech at sec.gov and will be posted on social media so that unfiltered critics can apply their editorial hacksaws to it.

You also can give me a call, send me an email, stop by my office, or provide feedback at FinHub. After all, I am very much a believer in the value of drawing on the creativity and ingenuity of as many people as possible.

That is why I find decentralized networks such a powerful phenomenon, and one that will allow society to benefit from the talents of people who—because of societal or geographic barriers—have heretofore been excluded.

I call particular attention to the definitions section of the safe harbor. I am a securities regulator, not a technologist, and am eager to learn how the definitions can be improved.

The challenge is accurately capturing the technology without baking-in terminology that will become outdated in a short period of time.

One struggle I have had in constructing this safe harbor is the appropriate scope. My core concern is for projects that are looking to build a decentralized network, but have difficulty bridging the legal gap.

Additionally, our staff has issued no-action letters to centralized networks.

While sales of tokens intended for these networks seem much less likely to implicate the securities laws, the existence of the no-action letters could be interpreted to suggest otherwise. Hence, I am suggesting that the safe harbor be available for these types of projects also.

Another unsettled matter is that the safe harbor could take the form of a rule or a Commission-level no-action position. In taking a no-action position, the Commission would pledge not to bring enforcement actions against project developers that fall within the parameters laid out in the position.

A no-action position may be preferable to a rule because it would not concede that the token sales it covers fall within or outside of our securities laws. Such grey areas are an appropriate place for no-action relief.

On the other hand, a rule-based approach would be more durable and would make clear that state laws do not apply. For purposes of this discussion, I will lay out the safe harbor as a rule.

Getting into the specifics of the proposal, the safe harbor would provide network developers with a three-year grace period within which they could facilitate participation in and the development of a functional or decentralized network, exempted from the registration provisions of the federal securities laws, so long as the conditions are met.

This objective is accomplished by exempting

(1) the offer and sale of tokens from the provisions of the Securities Act of 1933, other than the antifraud provisions,

(2) the tokens from registration under the Securities Exchange Act of 1934, and

(3) persons engaged in certain token transactions from the definitions of "exchange," "broker," and "dealer" under the 1934 Act.

The initial development team would have to meet certain conditions, which I will lay out briefly before addressing several in more depth.

First, the team must intend for the network on which the token functions to reach network maturity—defined as either decentralization or token functionality—within three years of the date of the first token sale and undertake good faith and reasonable efforts to achieve that goal.

Second, the team would have to disclose key information on a freely accessible public website.

Third, the token must be offered and sold for the purpose of facilitating access to, participation on, or the development of the network.

Fourth, the team would have to undertake good faith and reasonable efforts to create liquidity for users. Finally, the team would have to file a notice of reliance.

The first requirement—that the initial development team must intend for the network to reach network maturity within three years—is intended to focus project teams' minds.

At the end of three years, token transactions would not be securities transactions if the network has matured into a decentralized or functioning network on which the token is in active use for the exchange of goods or services.

To assess decentralization, the team must consider whether the network is not controlled and is not reasonably likely to be controlled, or unilaterally changed, by any single person, group of persons, or entities under common control.

The mere theoretical possibility of a 51% attack, for example, would not prevent a team from determining that the network is decentralized under this definition.

Nor would the participation of the team in a network alteration achieved through a predetermined procedure in the source code that involves other network participants prevent a team from determining that the network is decentralized.

To assess functionality at the end of three years, the team must consider whether holders can use the tokens in a manner consistent with the utility of the network.

For example, can holders use the tokens for the transmission and storage of value, to prove control over the tokens, or to participate in an application running on the network?

The tests laid out in the safe harbor are meant as proxies for the considerations raised in the SEC's Howey analysis and attempt to bring clarity on when a token transaction should not be considered a securities transaction.

These tests should be easier to pass at the end of three years than when the network is first launched.

Once the network cannot be controlled or unilaterally changed by any single person, entity, or group of persons or entities under common control, the token that operates on that network will not look like a security.

Even for a network that remains centralized—think of the networks outlined in the TurnKey Jet and Pocketful of Quarters no-action letters—once the tokens are actually in use to buy and sell the services for which they were intended, the securities laws will be clearly inapplicable.

Three years is a long time and token purchasers need certain protections during this grace period, which brings me to the second requirement detailing the disclosure that must be provided.

The disclosure requirement of the safe harbor addresses information asymmetry concerns and mandates that certain information be provided on a freely accessible public website.

The team launching a token project knows details about the project that would be useful for potential token buyers to know. Of primary importance is the source code and transaction history.

The safe harbor requires this information to be publicly available and encourages the development of a block explorer, or similar tool, for verifying the transaction history.

Token purchasers also need to understand the purpose and mechanics of the network.

For example, the team would have to explain the launch and supply process, including the number of tokens to be issued in the initial allocation, the total number of tokens to be created, the release schedule for the tokens, and the total number of tokens outstanding.

Public disclosure also would include information about how tokens are generated or mined, the process for burning tokens, the process for validating transactions, and the consensus mechanism.

The team also would have to explain the governance mechanisms for implementing changes to the protocol.

Another key disclosure would be the plan of development, including the current state and timeline for the development of the network that provides a roadmap to how and when the initial development team plans to achieve network maturity.

To demonstrate how realistic these plans are, a team could explain, for example, how the network development will be financed and who is on the development team.

To provide insight on the initial development team, the names and relevant experience, qualifications, attributes, or skills of each person that is a member of the team must be disclosed.

Required disclosure also includes the number of tokens owned by each member of the team, a description of any limitations or restrictions on the transferability of tokens held by such persons, and a description of the team members' rights to receive tokens in the future.

In addition, teams would need to disclose any time that a member sells five percent or more of her originally held tokens over any period of time, which would help to guard against fraud.

Additionally, team token sales could be an indication of flagging commitment to the project.

To further demonstrate their commitment to building a functioning network, teams will be required to update the posted disclosures to reflect any material changes.

Changes affecting the token economics, the network's functionality, or the team developing the network will be of great interest to potential users of the network.

A team committed to building a widely used network likely would provide these updates regardless of whether we mandated it.

The third condition is that the token must be offered and sold for the purpose of facilitating access to, participation on, or the development of the

network. This condition, along with the definition of token, is meant to clarify that the safe harbor is not appropriate for debt or equity securities masquerading as tokens.

The safe harbor's fourth condition requires the team to attest that it intends to, and will undertake, good faith and reasonable efforts to create liquidity for users.

To the extent the team attempts to secure secondary trading of the token on a trading platform, the safe harbor requires the team to seek a trading platform that can demonstrate compliance with all applicable federal and state law, as well as regulations relating to money transmission, anti-money laundering, and consumer protection.

Moreover, to alleviate existing regulatory uncertainty on the applicability of securities laws to the secondary trading of tokens, the safe harbor would exempt persons engaged in certain token transactions from the definitions of "exchange," "broker," and "dealer" under the 1934 Act.

Admittedly, the liquidity condition may surprise observers of SEC staff positions in which attempts to facilitate secondary trading have been viewed as indicia of a securities offering.

In the context of the safe harbor, by contrast, secondary trading is recognized as necessary both to get tokens into the hands of people that will use them and offer developers and people who provide services on the network a way to exchange their tokens for fiat or crypto currency.

To the extent it is aware, the team would disclose any secondary trading platforms on which the token trades.

The final condition is the need for the team to file a notice of reliance on EDGAR within fifteen days of the date of the first token sale in reliance on the safe harbor.

As part of the filing, a member of the team would have to attest that all the conditions of the safe harbor are satisfied.

The notice filing would also include the website where the required disclosure may be accessed. None of the disclosures required by the safe harbor would be provided in the notice filing on EDGAR.

Having outlined the conditions of the safe harbor, I would like to emphasize a few points concerning its scope. SEC enforcement has played an

important role in combatting fraud in connection with token sales. The safe harbor would not provide immunity from such actions.

First, the safe harbor would not be available to a team if one or more members of the team is subject to disqualification as a bad actor under the securities laws.

Second, the safe harbor would reserve the SEC's antifraud authority with respect to token sales under the safe harbor.

Although the safe harbor would preempt state securities laws, it would not stand in the way of state antifraud actions.

If anyone lied in connection with selling tokens pursuant to the safe harbor, the SEC or a state could bring an enforcement action.

This provision is not directed at teams that set forth a plan for a network and work earnestly toward building it, but fail to bring it to fruition.

Rather, it is designed to ensure that the SEC can bring suit against a team that sets out to defraud token purchasers by materially misrepresenting or omitting key information. We all know that there are plenty of those kinds of "projects" polluting the crypto space.

It is also important to note that the safe harbor would be available for tokens that were previously sold in a registered offering or pursuant to a valid exemption under the Securities Act.

These teams may need the safe harbor in order to permit secondary trading to occur and to distribute their tokens more widely into the hands of potential users.

Tokens that already are in widespread use on a decentralized network presumably are not securities and, therefore, would not need to take advantage of the safe harbor.

It is during the development phase that questions about the securities/non-securities line seem to be most difficult to resolve. Once a token network is up and running, few people would advocate application of the securities laws.

By essentially buying time for this question to be answered, the safe harbor makes it much more likely that the question as to whether something is a security can be answered in the negative.

Now that I have outlined the safe harbor, I suspect some of you are asking, "Who cares?" I get the point. I am one of five Commissioners. I cannot write rules unilaterally. However, to quote another of the Boss's songs: "you can't start a fire without a spark."

It does not hurt to get the ball rolling. People change their minds. Moreover, if we are going to do something like what I suggest today, I want to get it right.

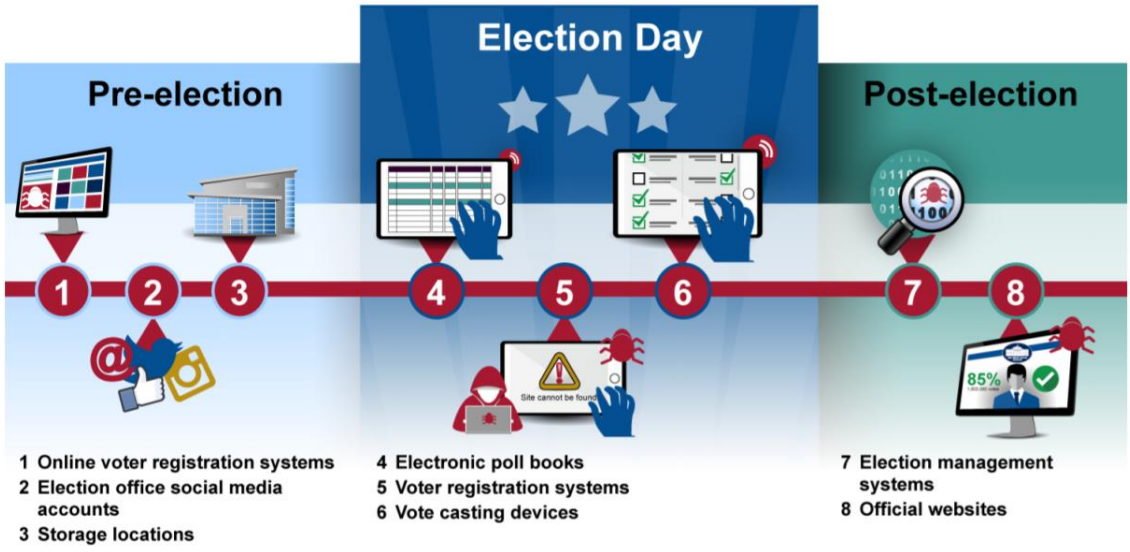
Getting it right means that I need people like those of you in the audience or reading this speech to weigh in and tell me what I have gotten right and what I have gotten wrong. Don't be that guy in New Jersey telling me I have to do this all by myself.

Number 5

Election security

DHS Plans Are Urgently Needed to Address Identified Challenges Before the 2020 Elections

Figure: Examples of Election Assets Subject to Physical or Cyber Threats



Source: GAO analysis based on information reported by the Department of Homeland Security, the Harvard University John F. Kennedy School of Government's Belfer Center for Science and International Affairs, and the Center for Internet Security. | GAO-20-267

Since the 2017 designation of election infrastructure as critical infrastructure, the Department of Homeland Security (DHS), through its Cybersecurity and Infrastructure Security Agency (CISA), has assisted state and local election officials in securing election infrastructure through regional support and assistance, education, and information sharing. Such efforts help state and local election officials protect various election assets from threats (see figure above).

In August 2019, the CISA Director identified election security as one of the agency's top five operational priorities.

CISA security advisors, who are located throughout the country, consult with state and local election officials and identify voluntary, no cost services that CISA can provide. According to CISA, as of November 2019, 24 cybersecurity advisors and 100 protective security advisors perform and

coordinate cyber and physical security assessments for the 16 critical infrastructure sectors, including the Election Infrastructure Subsector.

Technical teams at CISA headquarters generally provide the services, once requested.

To further assist state and local election officials, CISA conducted two exercises simulating real-world events and risks facing election infrastructure in August 2018 and June 2019.

According to CISA, the 2019 exercise included 47 states and the District of Columbia.

In addition, CISA has funded the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC).

According to CISA officials, the EI-ISAC is the primary mechanism for exchanging information about threats and vulnerabilities throughout the election community.

The EI-ISAC director reported that, as of November 2019, its members included 50 states, the District of Columbia, and 2,267 local election jurisdictions, an increase from 1,384 local jurisdictions that were members in 2018.

As a result of its efforts, CISA has provided a variety of services to states and local election jurisdictions in the past 2 years (see table).

Table: Number of Selected Cybersecurity and Infrastructure Security Agency Services Provided to States and Local Election Jurisdictions in 2018 and 2019, as of November 6, 2019

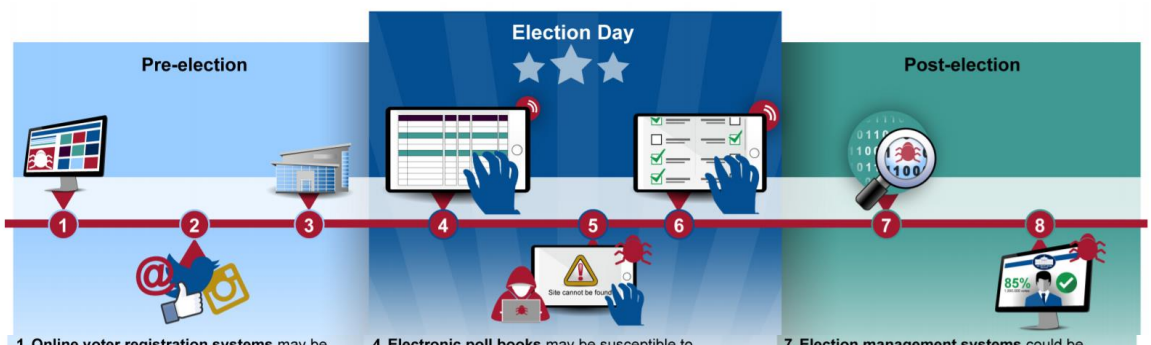
Service	States	Local election jurisdictions
Continuous scanning of internet-accessible systems for known vulnerabilities	40	161
Assessments of potential network security vulnerabilities	26	20
Remote testing of externally accessible systems for potential vulnerabilities	4	44
Assessments of states' and local jurisdictions' susceptibility to malicious emails	10	5
Educational posters on cybersecurity	19	1,202

Source: Cybersecurity and Infrastructure Security Agency. | GAO-20-267

State election officials with whom GAO spoke were generally satisfied with CISA's support to secure their election infrastructure. Specifically, officials from seven of the eight states GAO contacted said that they were very satisfied with CISA's election-related work.

Also, officials from each of the eight states spoke positively about the information that they received from the EI-ISAC.

Figure 1: Examples of Physical and Cyber Threats to the Election Infrastructure and Assets by Stage of the Election Process



1 **Online voter registration systems** may be susceptible to website spoofing as attackers can create a malicious copy of the official website to capture sensitive information or give voters the illusion that their information was updated. Targeted denial of service or outage attacks could prevent voter registration.

2 **Internal communication systems or election office social media accounts** could be compromised as attackers may use legitimate accounts from these systems to send out false information—such as false voting locations and inaccurate dates—to election officials, poll workers, or voters.

3 **Storage locations** may be vulnerable to physical tampering or destruction of voting equipment by attackers with malicious intentions.

4 **Electronic poll books** may be susceptible to compromise by malicious attackers who gain access to the poll books either using a wireless connection or because the physical device is not properly secured. A compromise to a poll book could allow attackers to manipulate the voter rolls—either deleting or altering existing voter registration data resulting in confusion when voters show up to vote on Election Day.

5 **Voter registration systems** access could be blocked and its data and backups could be encrypted or erased through ransomware, a type of malicious software, by attackers until a ransom is paid. This could also result in theft or irreversible encryption of voter registration databases and other sensitive records causing disruption to Election Day activities and potential decline in public trust.

6 **Vote casting devices** may be vulnerable to physical tampering using removable media or remotely using a wireless connection. A compromise to a vote casting device could allow a malicious actor to modify a vote on Election Day.

7 **Election management systems** could be compromised due to commercial software and hardware with security weaknesses or configuration errors in network connections. A successful attack could lead to manipulation of results during electronic transmission of vote tallies.

8 **Official websites** may be susceptible to compromise as attackers may replicate the official state or county website and post opposite results than are being reported—for instance, the winner of a particular race is now the loser.

Source: GAO analysis based on information reported by the Department of Homeland Security, the Harvard University John F. Kennedy School of Government's Belfer Center for Science and International Affairs, and the Center for Internet Security. | GAO-20-267

Further, officials from five states told GAO that their relationship with CISA had improved markedly since 2017 and spoke highly of CISA's expertise and availability.

To guide its support to states and local election jurisdictions for the 2020 elections, CISA reported that it is developing strategic and operations plans.

CISA intended to finalize them by January 2020, but has faced challenges in its planning efforts due to a reorganization within CISA, among other things.

In the absence of completed plans, CISA is not well-positioned to execute a nationwide strategy for securing election infrastructure prior to the start of the 2020 election cycle.

Further, CISA's operations plan may not fully address all aspects outlined in its strategic plan, when finalized.

Specifically, according to CISA officials, the operations plan is expected to identify organizational functions, processes, and resources for certain elements of two of the four strategic plan's lines of effort— protecting election infrastructure, and sharing intelligence and identifying threats.

CISA officials stated that CISA was unlikely to develop additional operations plans for the other two lines of effort—providing security assistance to political campaigns, and raising public awareness on foreign influence threats and building resilience.

To read more:
https://www.gao.gov/assets/710/704314.pdf

Number 6

Bank funding costs and solvency

Staff Working Paper No. 853 - Guillaume Arnould, Cosimo Pancaro and Dawid Żochowski, February 2020

High funding costs, if due to bank specific vulnerabilities, can erode banks' earnings and deplete banks' capital buffers in bad times or decelerate their build-up in good times.

Thus, high funding costs, when prompted by bank vulnerabilities, can have an adverse impact on banks' ability to withstand macroeconomic shocks and endanger the overall stability of the banking sector.

Indeed, the full pass-through of higher funding costs may be challenging in a non-monopolistic market if the increase in the funding costs is caused by bank idiosyncratic risks and does not reflect a general increase in interest rates.

To the contrary, a sector-wide increase in funding costs prompted by a rise in monetary policy rates would generally boost the profitability of banks which can increase their lending rates more than their deposit rates.

At the same time, if higher funding costs are passed through into higher lending rates, the real economy can also be adversely affected, by depressing the demand for new lending, prompting deleveraging and leading to lower economic activity.

Therefore, the dynamics of funding costs, their relationship with banks' characteristics and the related potential second round effects need to be considered in regular financial stability assessments and macroprudential stress testing frameworks.

Omitting them can largely underestimate banks' vulnerabilities.

The empirical literature generally shows that a negative relation between bank funding costs and solvency exists.

Bank funding costs are deemed to depend largely on the market perception of counterparty credit risk, which is driven by a wide range of banks' fundamentals including solvency, asset quality, profitability and liquidity.

Therefore, a worsening of banks' fundamentals and in particular weaker solvency may lead to higher funding costs.

However, a large part of the literature employs imperfect measures of bank funding costs.

Most of the existing studies on the topic use market-based measures.

These measures may not fairly represent the actual funding costs paid by banks.

The literature employing market-based measures also does not take into account the fact that different types of banks' liabilities might exhibit different sensitivities to stress conditions.

Other studies rely on balance sheet and P&L data to derive proxies of banks' funding costs.

Against this background, this paper studies the empirical relationship between banks' funding costs and their fundamentals.

In particular, it focuses on the relationship between banks' funding costs and solvency.

The analysis considers a large sample of euro area banks using two novel ECB proprietary datasets for banks' funding costs.

These datasets contain information on bank level senior bond yields and on bank level interest rates for term deposits and overnight deposits from customers.

Our analysis generally finds a significant negative relation between banks' solvency ratio and funding costs.

Moreover, it reveals that this relationship is non-linear, namely convex, for senior bond yields and interest rate for term deposits.

A decrease in the solvency ratio has a stronger impact on banks' senior bond yields and interest rates for term deposits for banks with a relatively lower solvency ratio.

The paper also identifies a realistic positive threshold for solvency at which the effect of solvency on senior bond yields changes sign and becomes positive. An increase in solvency leads to higher senior bond yields for banks with a relatively high solvency ratio.

This result suggests that it might be inefficient for banks to accumulate excessive capital. The paper also provides evidence that banks' senior bond yields are more sensitive to a change in solvency than deposit rates.

Indeed, the interest rates on the term deposits are less sensitive to changes in solvency than the senior bond yields.

Furthermore, the relationship between the interest rates on overnight deposits and solvency is negative but often not significant.

Banks' asset quality, profitability and liquidity seem to play only a minor role in driving funding costs while the ECB monetary policy stance, sovereign risk and financial markets uncertainty appear to be material drivers.

To read more:
https://www.bankofengland.co.uk/-/media/boe/files/working-paper/2020/bank-funding-costs-and-solvency.pdf?la=en&hash=4F66DCF4608E86B19CA9B5E0C920644A99ECFA0E

Number 7

Guidelines on outsourcing to cloud service providers now available for national supervisory authorities

The Guidelines shall provide guidance to market participants on how the outsourcing provisions set forth in the Directive 2009/138/EC, in the Commission's Delegated Regulation 2015/35 and in EIOPA's Guidelines on System of Governance need to be applied in the case of outsourcing to cloud service providers.

EIOPA developed these guidelines addressed to national supervisory authorities with the following objectives:

- To provide clarification and transparency to market participants avoiding potential regulatory arbitrages

- To foster supervisory convergence regarding the expectations and processes applicable in relation to cloud outsourcing

The use of cloud outsourcing is a common practice to all financial undertakings and not only to insurance and reinsurance undertakings. Moreover, the main associated risks are similar across sectors. Acknowledging these facts and recognising the potential risks of regulatory fragmentation, in developing these guidelines - in addition to the

(re)insurance provisions on outsourcing - EIOPA also considered the most recent guidance published by the European Banking Authority.

To read more:
https://www.eiopa.europa.eu/content/guidelines-outsourcing-cloud-service-providers_en

https://www.eiopa.europa.eu/sites/default/files/publications/eiopa_guidelines/final_report_on_public_consultation_19-270-on-guidelines_on_outsourcing_to_cloud_service_providers.pdf

Number 8

Office of Intelligence & Analysis
Strategic Plan for Fiscal Years 2020-2024.

Introduction, David J. Glawe, Chief Intelligence Officer, Under Secretary for Intelligence and Analysis.

I am pleased to publish the Office of Intelligence & Analysis Strategic Plan for Fiscal Years 2020-2024. This document provides a holistic approach that will guide the continued evolution of the Office over the next five years and serves as a foundational document for how DHS Intelligence executes its broad mission and vision.

Following the September 11th, 2001 terrorist attacks, the Homeland Security Act of 2002 created the Department of Homeland Security and the Implementing Recommendations of the 9/11 Commission Act of 2007 established the Office of Intelligence & Analysis as the first federal agency statutorily mandated to share intelligence with state, local, tribal, and territorial law enforcement, as well as the private sector—creating the necessity for a comprehensive approach and strategy to Homeland security.

I&A provides timely, actionable intelligence to a far-reaching base of customers and partners—from the DHS Secretary and Components, policymakers, and the Intelligence Community to an expansive network of state, local, tribal, territorial, and private-sector partners with both national and global influence.

Therefore, this strategy outlines a forward-leaning approach to provide dominant capabilities and anticipatory intelligence to meet the diverse needs of DHS partners, customers, and stakeholders.

The threat environment is never static, thus I&A will remain dynamic in its actions to combat the challenges of today, as well as the future, through partnerships, information sharing, and a concrete understanding of the evolving landscape at home and beyond our Nation's borders.

Terrorist networks continue operations to inspire and mobilize those in our country, transnational criminal organizations seek to exploit our borders, and state and non-state cyber actors target our critical infrastructure,

information networks, and the American people; all of these threats will be met with our most forceful and innovative efforts to repel all threats to the Homeland.

This strategy further develops I&A's contributions to national security as a member of the Intelligence Community while simultaneously outlining this Office's activities to integrate and strengthen Department of Homeland Security Intelligence capabilities.

To reiterate my commitment to empowering DHS Intelligence professionals, I&A developed this strategy using vital input of I&A employees as well as contributions from internal and external stakeholders.

I am committed to investing in the DHS workforce to develop premier Homeland Intelligence professionals, truly the most important factor in delivering superior intelligence capabilities in our fight against hostile actions that threaten American security, prosperity, and values that are the fabric of our Nation.

Thank you for your continued support as we work to foster a collaborative environment and continue to bridge the gaps between the federal government, the Intelligence Community, and our state, local, tribal, territorial, and private-sector partners.

It is imperative that we evolve together, as a unified community, to provide the most comprehensive and robust protection possible for the American people.

To read more:
https://www.dhs.gov/sites/default/files/publications/20_0206-oia-strategic-plan-fy20-24.pdf

Number 9

Improving 5G Network Security

DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

New program seeks to leverage open source software and systems to address security challenges facing 5G and future wireless networks

Emerging 5G mobile wireless networking technologies are slated to dramatically increase in both scale and speed, enabling much faster access to data collected from billions of connected devices.

This supercharged information highway is envisioned to play an important role across several industries, ranging from medicine to manufacturing.

Major advances in 5G, including new core network features will make it easier to customize the network at a wide variety of locations.

This new flexibility offers many benefits, but at the same time introduces novel security challenges.

Today's proprietary 5G technologies make it difficult to achieve the transparency necessary for security-related risk analysis and mitigation.

This lack of security assurance makes it harder to deploy these technologies for defense capabilities.

"As networks are simultaneously critical infrastructure and the means used for cyberespionage and cyberwarfare, finding ways to bolster their security is critically important," said DARPA program manager, Dr. Jonathan Smith. "The rapid increase in the scale of 5G networks, as well as issues from unmanaged or forgotten Internet of Things (IoT) devices and unwanted interactions between network slices, create security risks that must be addressed."

DARPA created the Open, Programmable, Secure 5G (OPS-5G) program to tackle many of the security challenges facing future wireless networks. OPS-5G will explore the development of a portable, standards-compliant network stack for 5G mobile networks that is open source, and secure by design.

The program seeks to enable a "plug-and-play" approach to various network software and hardware components, which reduces reliance on untrusted technology sources.

The goal of OPS-5G is to develop open source software and systems that can enable more secure 5G as well as future generations of networks beyond 5G.

The signature security advantage of open source (OS) software is increased code visibility, meaning that code can be examined, analyzed, and audited manually and, more fruitfully, with automated tools by multiple parties.

Another benefit is open source software's portability, which allows the software to run on both OS and proprietary hardware.

This decoupling of the hardware and software ecosystems makes it easier to introduce innovations while raising the difficulty of some malicious attacks.

Further, it helps open the 5G market to smaller players and innovators. However, creating open source software elements typically requires the collaborative development of well-defined standards.

The standards creation process can be slow and arduous – one that a rapidly-progressing technology such as 5G can't afford.

To help accelerate the development of 5G-relevant open source software from standards, OPS-5G will explore the use of machine translation to increase code development velocity and help make standards easier to understand.

One of the many benefits of 5G is powering a vast and growing ecosystem of IoT devices. The security across these devices, however, is disparate, as is their size, weight, and power (SWaP).

Today, IoT security features are viewed as optional, which does not bode well for their use within defense systems.

To bolster security around this growing mesh of technologies, OPS-5G will explore the development of cost-effective SWaP-conscious cryptography with scalable security protocols.

The program will look to existing technologies to support this process, like the many-to-many end-to-end encryption protocol developed by researchers at the University of California, Berkeley, called Joining Encryption and Delegation for IoT.

Network elements used to support virtualization and the 5G network concept of application-customized "slices" share resources to achieve cost-effective performance. Amongst other risks, this resource sharing creates potential timing channel vulnerabilities.

Opaque system ownership, operator policies, and software provenance also present security issues for 5G networks. Currently, a multitude of large vendors provide carrier hardware, software, node provisioning, and more to enable 5G technologies.

OPS-5G will explore breakthrough approaches for the enablement of secure network slices to provide security across the network resources provided by and shared with unknown entities. The program will explore novel ways to make trusted networks out of infrastructures with untrusted components.

Finally, OPS-5G will aim to address security challenges posed by 5G's programmability by hardening the execution. 5G is expected to have 60-600 billion nodes by 2023, which radically increases the risk of network attack.

To increase network resiliency and enable faster adaptation to threats, OPS-5G will explore the development of programmable elements of 5G specifically for defense.

Additional information is available in the OPS-5G Broad Agency Announcement, found at:
https://beta.sam.gov/opp/6ee795ad86a044d1a64f441ef713a476/view?keywords=DARPA&sort=-modifiedDate&index=opp&is_active=true&page=1

Number 10

Code repository used to host and distribute malware

National Cyber Security Centre

It is being reported that the code repository platform, Bitbucket, is being used by cyber criminals to host and distribute malware in a number of campaigns.

Criminals have been delivering an “unprecedented number of malware” via Bitbucket according to a report by Cybereason researchers.

The report:
https://www.cybereason.com/blog/the-hole-in-the-bucket-attackers-abuse-bitbucket-to-deliver-an-arsenal-of-malware

The malicious repositories mentioned in the linked blog post were deactivated within a few hours following communication between the researchers and Bitbucket.

Cybereason report that attackers create and cycle different accounts, which are then frequently updated to avoid detection..

Users that have downloaded cracked versions of commercial software like Microsoft Office and Adobe photoshop may have been affected.

The NCSC has produced guidance for mitigating the risk and impact of malware, but users should also ensure that they only download and install commercial software from trusted websites. You may visit:
https://www.ncsc.gov.uk/guidance/mitigating-malware

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.

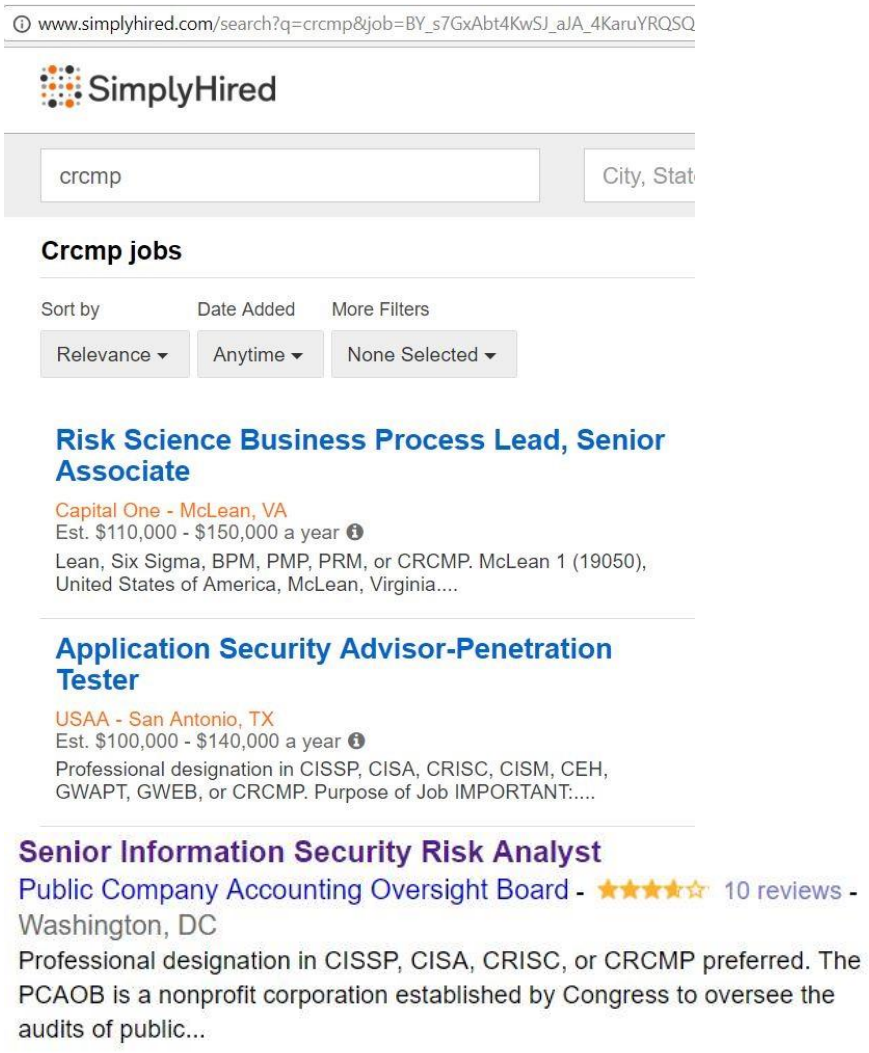
International Association of Risk and Compliance Professionals

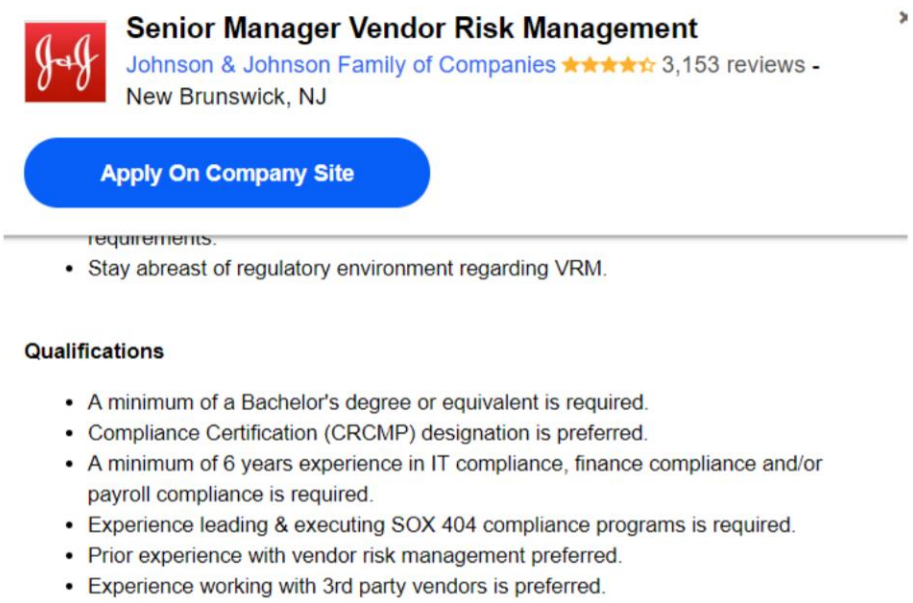
You can explore what we offer to our members:

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