STATEMENT OF

THOMAS MICHAEL FINAN
CHIEF STRATEGY OFFICER
ARK NETWORK SECURITY SOLUTIONS

BEFORE THE

U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON HOMELAND SECURITY

Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies

"The Role of Cyber Insurance in Risk Management"

Tuesday, March 22, 2016
311 Cannon House Office Building

Chairman Ratcliffe, Ranking Member Richmond, and Members of the Subcommittee, thank you for inviting me to address the role of cybersecurity insurance in risk management. I am the Chief Strategy Officer at Ark Network Security Solutions, a private company that provides software and services to accelerate standards compliance for enhanced security. Until this past December, I served as a Senior Cybersecurity Strategist and Counsel with the U.S. Department of Homeland Security's (DHS) National Protection and Programs Directorate (NPPD), where I launched and led DHS' Cybersecurity Insurance Initiative. I will describe the role that DHS has played in identifying and overcoming obstacles to a more robust cybersecurity insurance market. I will also discuss how the private-public engagement model that DHS has followed as a convener of the insurance conversation could be extended to address the cyber risk management needs of mid-size and small businesses nationally.

DHS' Cybersecurity Insurance Initiative

As a largely operations-focused organization, NPPD may not immediately come to mind as a likely candidate to lead a sustained discussion with stakeholders about cybersecurity insurance. NPPD has a more general mandate beyond its day-to-day cybersecurity mission, however, and its mission statement says it all:

> "*NPPD's vision is a safe, secure and resilient infrastructure where the American way of life can thrive. NPPD leads the national effort to protect and enhance the resilience of the nation's physical and cyber infrastructure."*

That means DHS must do more than just help its partners extinguish rapidly developing cyber risk "fires." It also requires DHS to think more strategically and to figure out what cyber risk fires – and what potential solutions to them – may be ahead and then determine how to address both as part of its overall resilience mission. Ultimately, DHS is in the risk management business. It is increasingly called to think about risk management not just three to five minutes, hours, or days ahead but – like its external partners – three to five years ahead.

Insurance, we learned, is a key part of that process. When we began DHS' inquiry into the cybersecurity insurance market, we asked whether cybersecurity insurance could – as a market force – raise the cybersecurity "floor" by getting more critical infrastructure owners to manage their cyber risk better in return for more relevant and hopefully more affordable policies. At the time, our point of reference was the fire insurance market. We knew that insurers had been very successful in identifying specific fire safety controls that today are not only conditions for coverage within fire insurance policies but also prerequisites for obtaining a building permit. Our hope was that brokers and underwriters together could help identify the cybersecurity equivalents of sprinkler and other fire suppression systems. What we discovered is that while they may get there one day, they are not there yet.

Challenges

From 2012 through 2014, DHS engaged a wide range of partners through a series of public workshops on the cybersecurity insurance topic. Our participants included brokers and underwriters, chief risk officers, chief information security officers, critical infrastructure owners and operators, and members

of the academic community. During the course of our conversations, we asked them whether now or in the future insurance could help incentivize better cyber risk management. DHS was especially interested in finding out if the market already provided coverage – or could eventually provide coverage – for physical damages and bodily injuries that might result from a successful cyber attack against critical infrastructure. What we heard back is that several major obstacles continue to prevent insurers from providing more cybersecurity insurance coverage – specifically, higher limits – than they currently do. Chief among them are:

- First, the market suffers from an ongoing lack of actuarial data. Unlike fire insurance, insurers do not have 100 years' worth of cyber loss data that they can use to build out new policies. This has inhibited them from providing more than the $10 to $15 million in primary coverage that they historically have offered customers for data breach and network security-related losses. Despite some recent progress, moreover, very few insurers provide discrete coverage for cyber-related critical infrastructure loss. When we asked why, the insurers explained that for obvious reasons, they do not receive claims against policies that do not yet exist. Without such claims, however, they have no way to build out the actuarial tables they need to expand their offerings. In short, they are left with little insight into the growing number of SCADA and other industrial control system attacks that are occurring worldwide. They insurers further advised that they similarly lack a consistent source of raw cyber incident data that they could alternatively use to get their underwriting bearings in this area.

- Second, brokers and underwriters cited the absence of common cybersecurity standards, best practices, and metrics as a further hurdle to a more robust market. They nevertheless cited the advent of the NIST Cybersecurity Framework in 2014 as a very positive development. Many advised that the Framework's common vocabulary for cyber risk management topics was helping them have more in-depth conversations with their current and potential clients about their cyber risk profiles than otherwise would be the case. They also told us that they would like to see tailored versions of the Framework emerge for each of the Nation's 16 critical infrastructure sectors that provide more particularized risk management information to their clients in those sectors. The ultimate utility of the Framework, they added, remains to be seen. Several underwriters explained that they continue to seek answers to two key questions: (1) are companies that use the Framework having a better cyber loss experience than their peers that don't; and (2) what Framework-inspired controls should be incorporated into cybersecurity insurance contracts as conditions for coverage – like sprinkler systems for fire insurance?

- Third, the workshop participants noted an ongoing lack of understanding about critical infrastructure dependencies and interdependencies as another major obstacle. Like most of the population, brokers and underwriters do not know much about how a cyber-related critical infrastructure failure in one sector might cascade across multiple other sectors. Until they have a better idea about how big and bad related losses might be – and where a strategically placed risk control might make a difference – they are reluctant to develop new insurance products to cover this loss category. Without more insight, one underwriter explained, one big loss affecting hundreds of clients could effectively put them out of business.

- Fourth, a final challenge to the cybersecurity insurance market is the ongoing failure by many companies to include cyber risk as part of their traditional enterprise risk management – or ERM – programs. Despite the growing threat, many companies continue to treat cyber risk as an IT problem, separate and apart from the other business risks they face. Without including cyber risk within existing ERM programs, however, they really are not "doing ERM." Consequently, they often are blind to their true risk profiles and may not be prioritizing their risk management resources most effectively.

Cyber Risk Culture

Given these obstacles, brokers and underwriters told us that they generally consider two major risk management factors when assessing a company's qualifications for coverage: its compliance with available cybersecurity standards and its risk culture. In so doing, they pay particular attention to the internal cybersecurity practices and procedures that a company has adopted, implemented, and enforced. Several underwriters advised that they focus primarily on risk culture when assessing a potential insured for coverage – leading them to draft custom policies for clients rather than more generic "template" policies that can be marketed more broadly. Regardless of their particular practices, practically all of the participants suggested that DHS should turn its attention next to how companies should go about building more effective cyber risk cultures.

This made a lot of sense. We started thinking: if a core group of brokers and underwriters is looking to how companies individually manage their cyber risk, then maybe we could discover some lessons learned that might be more broadly applicable to others. We therefore identified four "pillars" of an effective cyber risk culture that appeared to merit a deeper dive. Those pillars included the roles of:

- **Executive Leadership**. What should boards of directors be demanding – and doing themselves – to build corporate cultures that manage cyber risk well?
- **Education and Awareness**. What messages, training, and accountability mechanisms need to be in place internally in companies, among partnering companies, and at a national level to help create a culture of cybersecurity?
- **Technology**. How should technology be leveraged to encourage better cybersecurity practice?
- **Relevant Information Sharing**. Who within a company needs what information, and in what formats, to help drive more effective cyber risk management investments?

Several core conclusions emerged from our discussions:

- First, for many companies, the business case for more effective cyber risk management investment still has not been made. The key reason for this appears to be that cyber risk by and large has not been reduced to terms that non-technical business leaders can readily understand – namely, the financial costs of cyber events and the potential damages to reputation for failing to mitigate them adequately. Many of our participants suggested that to overcome this, companies should adopt ERM programs that incorporate cyber risk into the vast pool of other business risks they face.

- Second, many of our participants called for more research when it comes to the costs and benefits of existing and future cybersecurity solutions. Once corporate leaders engage, they explained, they will want to know what investments to make to best manage their cyber risk. In other words, which controls offer the most cybersecurity bang for the buck?

- Third, the participants explained that it probably is unrealistic to expect the insurance industry to come up with a one-size-fits-all suite of cyber risk controls that everyone should adopt in return for more coverage and (eventually) lower premiums. What the underwriters told us is that they typically do not spend weeks with potential insureds reviewing and red-teaming every aspect of their organizations to see what is happening with their information security. Moreover, they no longer subject corporate IT professionals to hundreds of detailed questions getting at the technical and human-based control aspects of this information. Instead, they usually survey the companies – asking just 20-25 questions directed at basic, high-level information security issues to eliminate only the most ill-prepared companies from coverage consideration.

This third point, however, does not mean that the insurance industry does not have an important cyber risk management role to play. On the contrary, what a growing number of strategically-focused brokers and underwriters look for during the underwriting process, separate and apart from the insurance application, is how well companies understand where they uniquely sit in the cyber risk landscape and what they are doing about their particular circumstances. Put simply, this means:

- Do they know what cyber incidents are actually happening to them based on their own data and reports from outside sources?
- Do they know – through public sources and private conversation – what kinds of cyber incidents are happening to other companies like them; and
- What cyber risk management investments are they making based on this information?

In other words, these brokers and underwriters are assessing whether a company exhibits an *engaged* cyber risk culture – one where corporate leaders support risk mitigation efforts aimed at the cyber risks most relevant to their companies. Such engagement serves as a critical point of differentiation between companies that represent a safer versus unsafe cyber risk.

Action Options

During DHS' fourth and final public workshop in April 2014, we asked our insurance participants how we could best help them work through some of the cybersecurity insurance market's persistent challenges. They identified three topic areas for further discussion:

- Cyber incident information sharing (as opposed to cyber threat sharing), with a specific focus on the value of creating an anonymized cyber incident data repository;
- Cyber incident consequence analytics; and
- Promotion of comprehensive ERM strategies that incorporate cyber risk.

When we asked how to prioritize this list, the insurance participants agreed that DHS should focus first on the concept of a cyber incident data repository – specifically, one that helps meet the cyber risk analysis needs of the insurance industry, chief information security officers (CISOs), chief security officers (CSOs), and other cybersecurity professionals.

From the start, the brokers and underwriters described a repository notionally as a place where companies could anonymously share their cyber incident data. That data, they explained, could then be aggregated and analyzed to increase awareness about current cyber risk conditions and longer-term cyber risk trends. They explained that this information could benefit not only the insurance industry with its risk transfer efforts but also CISOs, CSOs, and other cybersecurity professionals with their complementary cyber risk mitigation efforts. The brokers and underwriters emphasized that these professionals should be central to any future repository discussion. They felt strongly that if the men and women on the front lines of cybersecurity are not "bought in" on the idea, then all the talking in the world would be for naught. We agreed and endeavored to engage not only insurance experts but also these day-to-day practitioners who had hand-on knowledge about cyber incidents and the kinds of analysis that would help them better prepare, respond, and recover from them. The results from our initial follow-up conversations testing the waters were promising:

- From the insurance side, we heard that a repository could help the industry build up the information stores it needs to better understand the impacts of cyber events, their frequency, and the optimal controls for mitigating particular kinds of cyber incidents. Various brokers and underwriters told us that this knowledge could help them scope and price policies that contribute more effectively and more affordably to a company's overall corporate risk management strategy. Many of them believed, moreover, that a repository one day could help them provide more cybersecurity insurance at lower rates to clients that invest in so-called "best-in-class" controls. Repository-supported analysis, they explained, would be essential for identifying those controls.

- For their part, the CISOs and CSOs told us that repository-supported analysis could help them conduct much needed peer-to-peer benchmarking and other activities that could bolster their in-house cybersecurity programs.

- Cybersecurity solutions providers reported that they also have a critical stake in any future repository. They explained that repository-supported analysis would likely influence how the market for new solutions develops. Specifically, they told us that greater knowledge about longer-term cyber incident trends will inform the kinds of products and services that they create to meet the risk mitigation needs of clients across every industry sector.

The CIDAWG

In late 2014, DHS approached the Critical Manufacturing Sector Coordinating Council (CMSCC) to sponsor and identify willing CISOs to participate in the newly initiated Cyber Incident Data and Analysis Working Group (CIDAWG). The CMSCC was immediately supportive of the repository concept and named several CISOs to the group. DHS also was very fortunate to be joined by a number of brokers and

underwriters from the previous public workshops who had been strong proponents of the idea. At the outset, the CIDAWG included about 10 brokers and underwriters that were among the top thought leaders in the cyber insurance industry. DHS paired them with approximately 25 CISOs, CSOs, and other cybersecurity professionals to enter into a sustained dialogue about four main agenda items:

- The value proposition for a cyber incident data repository;
- The data categories necessary to support repository-supported analysis that helps companies manage their cyber risk better;
- How to encourage the voluntary sharing of cyber incident data repository into a repository; and
- How a repository should be structured in any proof of concept stage.[1]

To be clear, DHS is not building a repository. Instead, it is creating a safe space for people to discuss how a repository notionally should come together as a place where companies feel comfortable sharing their cyber incident information anonymously. To do so, DHS established several ground rules that have been critical to the success of the project to date:

- During DHS' previous public workshops, we learned that hosting our discussions on a confidential basis helped promote rigorous debate. We therefore followed suit with the CIDAWG and held all of our meetings under the auspices of the Critical Infrastructure Partnership Advisory Council (CIPAC), a mechanism that allowed us to keep them closed to the public. We likewise strictly enforced the Chatham House Rule to ensure a constant flow of conversation among CIDAWG participants.

- At all times, DHS also tried to be sensitive to the demands that the CIDAWG's work placed on its members. They were located all over the country across every time zone, and we recognized that their time was extremely valuable. To that end, we scheduled CIDAWG teleconferences for up to twice a month, for up to two hours at a time. While we scheduled two in-person meetings for the group in the Washington, D.C., area during the year, we did so only with the participants' consent. We also provided them with several months of lead time so they could provide notice to their employers and budget and plan for the meetings accordingly.

The Value Proposition

The CIDAWG's first topic was the value proposition for a repository. How could it help advance the cause of cyber risk management and what kinds of analysis would be most useful to the cybersecurity industry, to CISOs and CSOs, and why? The brokers and underwriters responded that a repository could help facilitate the development of cybersecurity best practices that insurers should require within their policies as conditions for coverage. The CISOs and CSOs added that a repository could provide the data needed for more insightful peer-to-peer benchmarking that could help justify – or modify – existing

[1] The CIDAWG's conclusions about the first three of these topics are included in a series of white papers available on DHS' Cybersecurity Insurance webpage, accessible at https://www.dhs.gov/cybersecurity-insurance.

cybersecurity investments. As they explained, knowing how a company's peers are faring on the cyber risk management front and how it compares to them goes a long way toward making the business case for needed funding. Both groups noted that repository-supported analysis likewise could help the cyber risk management community identify longer-term cyber risk trends, allowing for new kinds of cyber risk forecasting that could help further inform cybersecurity budgets.

In June of 2015, the CIDAWG completed its first white paper that captured the group's core findings. The paper detailed six major value proposition categories for the kind of repository that they were envisioning. Specifically, they believed that it could help by supporting analysis that:

- Identifies top cyber risks and the most effective controls to address them;
- Informs peer-to-peer benchmarking;
- Promotes sector differentiation;
- Supports cyber risk forecasting, trending, and modeling; and
- Advances cyber risk management culture.

The Data Categories

In September 2015, the CIDAWG released its second white paper about the cyber incident data categories that contributors should share into a repository to deliver on that value. Early on, the brokers and underwriters explained that they wanted to know more about the types of cyber incidents that are happening; their severity, impacts, and timelines; the apparent goals of attackers; effective response techniques; involved parties; and risk controls that are making a difference. During the course of our conversations, we asked the CIDAWG participants to flesh all this out by telling us what value each data category potentially brings to a better understanding of cyber incidents; what each one actually means and to whom; which data categories were the greatest priority, to which stakeholders, and why; and which of them are actually accessible,

What was particularly gratifying to see was how the CIDAWG members came to view each data category in relation to at least one of the six value proposition categories that they had previously identified. During their deliberations, they asked themselves, "How does this particular data category deliver on the value that we're all seeking together?" After three months of work, this resulted in a very compelling final list. While the brokers and underwriters were the first to offer up their ideas – they came up with 16 of their own data categories – the discussion did not stop there. The CISO and CSO participants identified their own set of nine data categories that they believed were essential from a cybersecurity operations perspective. After sometimes intense debate and discussion, the CIDAWG completed a final list – coincidentally, of 16 consolidated data categories – that are a priority for both the insurance industry and cybersecurity professional community alike. They include:

- Type of Incident;
- Severity of Incident;
- Use of a Cyber Risk Management Framework;
- Incident Timeline;

- Apparent Goal(s) of Attackers;
- Contributing Causes;
- Specific Control Failures;
- Assets Compromised or Affected;
- Types of Impacts;
- Incident Detection Techniques;
- Incident Response Playbook;
- Internal Skills Sufficiency;
- Mitigation and Prevention Measures;
- Costs;
- Vendor Incident Report; and
- Related (Contextual) Events.

Overcoming Obstacles

As a next step, the CIDAWG addressed how private companies and other organizations could be encouraged to voluntarily share all this information into a repository. To prepare for this conversation, the CIDAWG hosted several experts who described already existing and ongoing information sharing efforts. Our hope was that the CIDAWG would use these models to propose similar approaches for an anonymized cyber incident data repository:

- Representatives from the Department of Defense (DoD) provided a very helpful overview of some of the information sharing work that is being done by Defense Industrial Base or "DIB" companies. Specifically, DoD shared its insight into how DIB companies have created a trusted information sharing environment by adopting a unique way of anonymizing data and using Non-Disclosure Agreements.

- The MITRE Corporation likewise detailed the progress of the Aviation Safety Information Analysis and Sharing System – the so-called "near-miss" database – that MITRE established and runs in partnership with the aviation sector. Specifically, the representative outlined the best practices MITRE had developed to promote the anonymized sharing of near-miss information by pilots, flight attendants, ground crews, and others to enhance flight safety.

- The Alliance for Telecommunications Industry Solutions (ATIS) also shared its experiences in creating a trusted environment for the confidential sharing of highly sensitive network outage information.

In December 2015, the CIDAWG released its third white paper that identified eight perceived obstacles to repository sharing and potential ways to overcome them, many of which had been inspired by these outside group briefings. The obstacles included:

- Assuring Anonymization (prevent data from being traced back to a particular contributor);
- Ensuring Data Security (protect the repository itself from breaches);
- Cultural Challenges and Regional Differences (avoid potentially skewed data);

- Perceived Commercial Disadvantage to Participating in a Repository (address concern that participation could negatively impact business operations);
- Internal Process Hurdles to Participation (find ways to work through key reviewers);
- Perceived Value of Participation (evangelize the bottom line benefits of participation);
- Assuring Appropriate, Adequate, and Equitable Participation (develop a series of benefits available only to repository contributors); and
- Technical Design Issues (make the repository easy to use).

Outcomes

DHS and the CIDAWG are currently planning a public workshop in April 2016 to obtain feedback on the CIDAWG's white papers. Specifically, they are planning to dive into the 16 cyber incident data categories in order to validate them. They also plan to assemble a panel of experts who will offer recommendations about how a repository should function during any future proof of concept stage.

While the CIDAWG will likely make a number of recommendations for next steps based on this input, one of them already is clear: the Federal Government should not actually own or operate the repository. While the CIDAWG members reported that they would welcome data from Federal agencies into a repository, they felt strongly that the private sector should find its own way during a future repository implementation stage. At the same time, however, they expressed great interest in DHS continuing to convene the CIDAWG and any other working groups to take the work to the next level.

Cybersecurity for Mid-Size and Small Businesses

As with the CIDAWG, DHS' convening power could provide tremendous benefit when it comes to helping mid-size and small businesses struggling with their cybersecurity efforts. By some estimates, the cybersecurity insurance market today is growing at 30% a year. Brokers and underwriters alike agree that mid-size and small businesses represent the next cohort of clients that they need to engage in order to sustain that growth. While the market already offers cybersecurity policies geared to these enterprises, they face the same challenge as their larger counterparts: managing their cyber risk well over time in order to qualify for meaningful coverage. Unlike those counterparts, however, mid-size and small businesses tend to have weaker security that makes them much easier to attack successfully. It likewise makes them a prime launching point for attacks against others. As the "Target" data breach in 2013 starkly demonstrated, a cybersecurity failure by one small business – in that case, a heating, ventilation, and air conditioning (HVAC) vendor – can impose hundreds of millions of dollars in lost income and related litigation and settlement costs.

Mid-size and small businesses are falling behind for several reasons. As an initial matter, most lack the budgets, expertise, staff, and time to adequately and consistently address their cyber risks. Many have concluded – wrongly – that their relative anonymity protects them from breaches and cyber-related business interruption events. Given competing business concerns, moreover, still others have simply chosen not to prioritize cyber risk management very highly. Mid-size and small businesses accordingly often fail to comply with common cybersecurity standards that promise real protection through the

deployment of appropriate security infrastructure. A growing number, for example, use the cloud as a cost-saving measure for their transactions, unfortunately without strong encryption technology in place. As a result, these businesses represent the weakest links in the global supply chain, making them less attractive business partners.

Large companies have awoken to this problem and are increasingly inquiring of their current and potential supply chain partners about the effectiveness of their cyber risk management programs. In many cases, the less-than-stellar answers they receive present a quandary that raises difficult questions:

- How should large companies define and measure "reasonable cybersecurity" for the mid-size and small companies with which they partner?
- Would imposing their own, potentially more costly cybersecurity requirements effectively put those enterprises out of business?
- Should large companies sever business ties with mid-size and small vendors and suppliers in favor of others that in reality may be no more "cyber secure"?
- How and how often should they verify whether a mid-size or small business is actually complying with cybersecurity requirements over time and "course adjusting" their cyber risk management investments in response as necessary?
- When does the risk of transacting business with a less-than-secure enterprise outweigh a large company's absolute need for a unique service or product that that enterprise provides?
- Does a cyber insecure organization provide products or services at such a competitive rate that a larger company should continue to take a chance through continued partnership?

Part of the answer to these questions is that cybersecurity in today's hyper-connected world is not like the television game shows "Weakest Link" or "Survivor" where mid-size and small businesses should somehow be eliminated or voted off the island automatically because they suffer a breach or other damaging cyber event. The fact of the matter is that all businesses – large, mid-size, and small – are linked through the supply chain. They all are on the same island. Accordingly, they need to work with each other to survive and thrive in today's fast-evolving cyber risk environment. Cybersecurity collaboration among these enterprises has never been more essential.

DHS should consider convening an ongoing conversation focused on this topic. The CIDAWG provides an excellent model for how different cybersecurity stakeholders – brokers, underwriters, CISOs, CSOs, and other cybersecurity professionals – can be drawn together to confidentially discuss shared cyber incident data and analysis requirements. A similarly structured dialogue could focus large, mid-size, and small business attention on the specific approaches and support structures needed to advance the cybersecurity performance of all partners across the supply chain.

Brokers and underwriters would have particularly insightful perspectives to share on this topic given their growing interest in encouraging better cybersecurity among the mid-size and small businesses that will comprise a sizable portion of their future client base. A new working group could assess, for example, how more effective cybersecurity collaboration among all supply chain partners – through initiatives like cybersecurity expert exchanges, best practice knowledge sharing, compliance automation,

and coordination of cybersecurity investments – might help establish mid-size and small businesses as more attractive insurance risks. As brokers and underwriters learn more about which cyber risk controls work for larger companies, they could become a powerful voice regarding which ones should be prioritized and adapted to the needs of the vendor and supplier community. Over time, the group's recommendations could be developed, shared, and updated through a standing private-public partnership effort dedicated to this issue.

Thank you. I am happy to answer any questions you may have.