AUBURN UNIVERSITY

CENTER FOR CYBER AND HOMELAND SECURITY

Strengthening Defense Mission Assurance Against Emerging Threats

Mission Assurance Policy Forum
Summary of Proceedings
May 2019

This publication is the exclusive work product of the Center for Cyber and Homeland Security. This forum and publication of this document was made possible thanks to the technical and finacial support of ICF Inforporated LLC of Fairfax, Virginia.

AUBURN

UNIVERSITY

CENTER FOR CYBER
AND HOMELAND SECURITY

cchs.auburn.edu

ABOUT US

The Center for Cyber and Homeland Security at Auburn University is a nonpartisan think tank that works to develop innovative strategies to address current and future threats to the United States. We convene leading experts and practitioners for executive-level events, publish policy-relevant analysis, and provide expert testimony to Congress on critical issues and challenges related to cybersecurity, critical infrastructure, counterterrorism, and homeland security. The Center is part of the McCrary Institute for Cyber and Critical Infrastructure Security, and drives the policy component of the Institute's work.

ICF makes big things possible

ICF is a global consulting services company with more than 5,500 specialized experts, who are not typical consultants. They combine unmatched expertise with cutting-edge engagement capabilities to help clients solve their most complex challenges, navigate change, and shape the future.

ICF's Enterprise Cybersecurity and Resilience (ECR) practice provides an integrated suite of adaptive risk management and resilience solutions. ECR takes a holistic, risk-informed approach to helping clients identify, prioritize, and mitigate threats and hazards across critical infrastructures, networks, and systems.

ICF is proud to be a corporate sponsor of the Center for Cyber and Homeland Security at Auburn University.

FOREWORD

AUBURN UNIVERSITY

CENTER FOR CYBER
AND HOMELAND SECURITY

On March 20, 2019, the Auburn University Center for Cyber & Homeland Security (CCHS) convened a Policy Forum on Strengthening Defense Mission Assurance Against Emerging Threats. The Forum was made possible through the technical expertise and support of our sponsor ICF Incorporated LLC, of Fairfax, VA, and by Sonecon LLC of Washington, DC.

Three panels addressed the evolving character of conflict and how potential adversaries may employ hybrid and asymmetric means not only to jeopardize or disrupt the execution of defense missions abroad but also the stability and security of the homeland. Through panel discussions and audience participation, the Forum explored the accelerating need for DOD to partner with other federal departments and private sector industry to help strengthen mission assurance and better protect a homeland that is no longer the sanctuary it once was.

In a set of panel summaries, CCHS shares the content of these Forum discussions and points to a way ahead for a more comprehensive, collaborative, whole-of-nation approach to mission assurance. That approach must not only encompass the protection of our Nation's war-fighting capability but the civilian critical infrastructure, networks, and systems on which our military might, national economic prosperity, and democratic way of life so greatly depend.

Following a keynote address by the Honorable Kenneth Rapuano, Assistant Secretary of Defense for Homeland Defense and Global Security and subsequent opening discussion, the Forum program was broken up into three facilitated panel exchanges as follows:

- Mission Assurance as a Component of Warfighting;
- Mission Assurance Civil/Military Interdependencies; and
- Industry/Government Interchange and Collaboration.

This report is produced in and reflective of the spirit of CCHS as a nonpartisan think tank that works to develop innovative strategies to address current and future threats to the Nation. CCHS regularly convenes leading experts and practitioners for executive-level events, publishes policy-relevant analysis, and provides expert testimony to Congress on critical issues and challenges related to cybersecurity, critical infrastructure protection, counter-terrorism, and homeland security. The Center is part of the McCrary Institute for Cyber and Critical Infrastructure Security, and drives the policy aspects of the Institute's work.

Hopefully, this Report provides some of what is needed to tackle the hard issues and assist our policymakers and decision-makers, as they translate concepts into lasting capabilities in order to enhance our national and homeland security posture. We are very grateful to the senior officials and panelists who contributed valuable time and expertise to this Forum —

including of course our esteemed colleagues at the Department of Defense. Though not for specific attribution, their collective views, and the views of the members of the audience, as expressed during the course of the Forum, are faithfully represented in the pages that follow.

Finally, special and hearty thanks are due to ICF senior vice president John Paczkowski and Sonecon managing director Dr. Paul Stockton for their unflagging and energetic commitment to the design and execution of the Forum, and their insights and analysis throughout. In addition, grateful thanks are also due to our valued support team members who were critical to the planning and implementation of this initiative, including ICF senior vice president Mike Pampalone, Sonecon director of security research & analysis Rob Denaburg, CCHS deputy director Sharon Cardash, and CCHS staff assistant Matthew Edwards.

Frank Cilluffo
Director, McCrary Institute for Cyber and Critical Infrastructure Security, and
Director, Center for Cyber and Homeland Security
Auburn University

TABLE OF CONTENTS

MISSION ASSURANCE POLICY FORUM

SUMMARY OF PROCEEDINGS

BACKGROUND

As our Nation continues to deal with the threat of transnational terrorism, we are now confronted with a reemergence of peer nation-state competitors whose warfighting doctrine increasingly demonstrates the intent to employ hybrid and asymmetric methods, including economic means and other efforts short of war, to achieve their economic, political, and military objectives. Combatant Commanders (CCDRs) are thus faced with an intensifying and more complex set of risks to their missions, not only within their regions or assigned areas of responsibility but stretching back to and including the homeland. That homeland is no longer uncontested but now a part of larger multi-domain battlespace. Disrupting or destroying mission-critical infrastructure, systems, and networks anywhere in that expanded battlespace could offer our adversaries an indirect and potentially devastating means to degrade the mobility, sustainment, and lethality of U.S. combat forces. It could also cripple or deny access to the facilities and critical infrastructure of allied and host nations or that of the homeland to a level that weakens our individual and collective ability and will to fight.

Since publication of its Mission Assurance (MA) Strategy, the U.S. Department of Defense (DOD) has taken far-reaching steps to protect its mission essential functions and critical assets. Likewise, following the issuance of the National Infrastructure Protection Plan (NIPP), the U.S. Department of Homeland Security (DHS), in partnership with other federal departments and the private sector, has made complementary efforts to enhance the resiliency of civilian critical infrastructure and cyber networks. However, likely adversaries are developing and refining evermore sophisticated means to exploit, disrupt, and/or destroy the energy, communications, logistics, transportation, water, and other key functions and assets on which both the American people and their military so greatly depend. The very nature of these risks and associated interdependencies means there is no longer a clear distinction between the "home and away" games, as the once sharper lines dividing national security, homeland defense, and homeland security have begun to blur. It is thus time to reexamine DOD's MA posture in concert with its interagency and industry partners and explore a more robust whole-of-nation approach to national security and resilience.

This forum was intended to help promote the importance of more fully incorporating MA considerations in operational planning by the warfighting combatant commands and the significant need to foster a joint MA mindset among supporting service components, agencies, and civilian partners. It was also designed to identify opportunities for more complete consideration of cross-sector civil/military interdependencies and the stronger integration of cybersecurity threats into regional and system-wide risk assessments, to include those conducted by DOD and DHS within the homeland. Finally, Forum participants were encouraged to suggest actions DOD and its partners might take to advance the evolution of MA programs, especially as they pertain to fostering greater civil/military collaboration.

OPENING DISCUSSION

Speakers/Panelists
Kenneth Rapuano, Assistant Secretary of Defense, HD&GS, DOD

Moderator
Frank Cilluffo

Most of the infrastructure, networks, and systems that DOD relies on to support its critical missions are owned and operated by the private sector, and thus outside departmental control. Threats to this civilian support structure are on the rise and, given DOD's tremendous dependence on mission critical assets in civilian hands, we cannot de-couple them from the Nation's warfighting capabilities. DOD and its partners are making progress on MA initiatives, but much more action is needed. The purpose of this Forum is therefore to "translate the nouns into verbs," and improve DOD engagement with civilian agencies, such as DHS, and private sector infrastructure owners and operators. It is vital that we not simply "admire the problem." The goal here is to advance a set of actionable solutions to these enduring challenges. A major paradigm shift is needed to address rapidly evolving threats and bolster defense of the homeland, to include its warfighting capability.

The Homeland is No Longer a Sanctuary.

During the Cold War, the U.S. was facing the threat of Soviet and Chinese nuclear attacks. While daunting, these were tangible albeit catastrophic threats, held in check largely by the potential for mutual destruction. With the fall of the Soviet Union and the ending of the Cold War, we experienced a period of escalating activity by transnational terrorist groups. In the wake of 9/11, these and other non-state actors were the major focus. While they could carry out attacks with grave human, economic, and political consequences, not to mention inciting the two longest wars in our Nation's history, they presented a relatively limited threat to DOD MA.

Today, the greatest threats to the U.S. homeland have shifted back to near-peer adversaries. As noted in the National Defense Strategy (NDS), "the homeland is no longer a sanctuary." These adversaries are applying major resources to developing military capabilities and new technologies to challenge us in all key domains; sea, air, land, space, and cyber. We must not be sanguine about either the national security implications of risks to civilian critical infrastructure or the vulnerability of our military's support architecture and its evermore complex networks and weapons systems. The same is true for our allies and host nations on which our warfighters so greatly depend.

We are at Risk from New Threats in the Grey Zone.

Our Nation's conventional military superiority is deterring our adversaries from challenging us directly on the traditional battlefield. Instead, they are increasingly supplementing conventional military force structure and equipment with the pursuit of new asymmetric capabilities in the "grey zone." Competitors are stealing intellectual property (IP), conducting influence operations targeting the American public and our allies, and carrying out malicious cyberattacks that create vulnerabilities within critical infrastructure systems, to include those on which the lethality, mobility, and resilience of our military forces so greatly rely. None of these alone may constitute an act of war, but each of them threatens national security and, taken together, they constitute a

persistent campaign to degrade and possibly even cripple our ability to project force when and where required in response to a military provocation.

The objective of our adversaries is ultimately to undermine the U.S. economy, our military strength, and the public's sense of security and confidence in its government, slowly eroding not only American military supremacy but also our cherished democratic institutions. A large number of small attacks can have cumulative, strategic consequences – "death by a thousand cuts." These attacks are more probable given the currently low risk and lack of response our adversaries perceive in carrying them out. If they can, these opponents are attempting to achieve their strategic, economic, and political objectives without firing a shot, and without risking escalation. However, if all-out conflict occurs, they will attempt to ensure their victory by using these asymmetric capabilities to cripple the critical infrastructure on which DOD relies.

Exploitation of Interdependencies Can Have Major Consequences.

DOD and its partners must not only work more closely together to build capabilities to deter unconventional attacks against the homeland but those same partners must also work more closely with DOD to help it protect warfighting capability that extends all the way forward from the homeland into the battle zone. This requires an approach to MA that assumes – while the U.S. cannot defend every important asset – DOD's prioritized approach to protecting Defense Critical Infrastructure (DCI) will ensure that sufficient warfighting capability survives to both defend the homeland and defeat any adversary. That said, we cannot yet affirm with great confidence that we have achieved that goal. Threats to military and civilian infrastructure multiply and evolve daily, challenging our ability to keep pace.

DOD is getting much better at securing the physical infrastructure and assets that it owns and is devoting considerable new resources to building resilience into its cyber networks and evaluating cyber risk in its mission assurance assessments. However, the Department has much less visibility on and influence over the identification and mitigation of risks to mission critical physical infrastructure and cyber networks in civilian hands – assets "outside the wire." Whether directly or indirectly associated with our Nation's warfighting capability, infrastructure and cyber interdependencies and the cascading effects of an attack on communications, energy, transportation, and Defense Industrial Base (DIB) supply chain assets can have major consequences for military operations. This is as true for the infrastructure of allied and host nations as it is for that of the homeland.

We Need a Better Framework for Civil-Military Collaboration.

There is no daylight between the armed forces and industries of our most threatening near-peer adversaries as they work with and support each other to gain both competitive and military advantage. That is why, now more than ever, U.S. government and private sector leaders must

find new ways to strengthen and accelerate collaboration for mission assurance. In response to these challenges, DOD is working across the federal interagency, private sector industry, and other stakeholders to share threat and criticality information, identify priorities to improve collective resilience, and ensure its various partners meet requisite security standards. Those efforts are gaining momentum but are still in a relatively nascent stage and must be expanded and made more robust to effectively counter the dynamic threats now before us.

As it has evolved to date, there are four basic pillars or phases of the Defense MA Construct:

- **Identify –** DOD and its partners are engaged in a continuous process of identifying and evaluating the criticality of assets and capabilities on which Defense missions depend.

  Note: For Defense Critical Infrastructure (DCI) that it does control, the Department is increasingly working with industry owners and operators to accomplish the same goal. A key principle being: *"When you try to defend everything, you defend nothing."*

- **Assess –** Once priorities based on criticality are set, DOD assesses risks (likelihood and consequence) to the mission from loss of key assets, networks, systems, and platforms.

- **Manage –** Risk mitigation investments are then considered along with alternatives to otherwise manage risk by avoiding, deferring, or transferring its potential. This step includes an assessment of adversary capabilities to ensure best return on that investment.

- **Monitor –** It is essential for government and private sector infrastructure owners and operators both inside and outside the fence line to observe and report on incidents and newly-identified vulnerabilities. Timely incident reporting is critical for managing risks.

The four pillars of MA, with supporting detail and associated processes, are provided in the DOD Mission Assurance Strategy (2012), DOD Directive 3020.40 *"Mission Assurance (MA),"* and DOD Instruction 3020.45 *"Mission Assurance (MA) Construct."*

Asymmetric Threats Demand a Whole-of-Nation Effort.

The cycle of risk management represented in the four pillars of the MA construct is not unlike the framework for protection of civilian critical infrastructure established by DHS. That similarity notwithstanding, we have yet to fully synchronize approaches to more effectively share our respective understandings of the threat; coordinate in the identification and prioritization of critical infrastructure assets, networks, and systems with national security significance; and assess associated criticality, interdependencies and risks. Nor have we fully harmonized efforts to mitigate, avoid, defer, or transfer the potential consequences of those risks from a whole-of-nation perspective. Though major progress is being made, and DOD and its civilian agency and industry partners are working more closely together, the threat continues to accelerate.

Nowhere is the need for a true "whole-of-nation" approach clearer than in the cyber realm. In cyberwarfare, "whole-of-nation" must be much more than a catchy buzz phrase. DOD has significant capabilities and authorities for cyber conflict, but effective responses will require significantly broader interagency and national coordination. The Nation's response to a major cyber-attack on critical infrastructure will not always be in the cyber realm. The U.S. government (USG) needs to hold the adversary accountable and extract penalties in whatever way is most effective. It is "rarely going to be cyber in kind."

PANEL #1
MISSION ASSURANCE AND WARFIGHTING

Speakers/Panelists
Charles Kosak, Deputy Assistant Secretary of Defense, DC&MA, DOD
Lt. Gen. Reynold Hoover (Ret), former Deputy Commander, USNORTHCOM
Maj. Gen. Joseph Whitlock, Director, Army Protection (G-34), HQDA
Dr. Richard Andres, Professor, National War College

Moderator
Dr. Paul Stockton

The U.S. homeland is no longer a sanctuary. Our adversaries have given us very clear indications of their intent to use hybrid and asymmetric means to attack our Nation and its interests, at home and abroad, when and if they so choose. They have developed associated doctrine and are advancing sophisticated campaign plans to actively target U.S. critical infrastructure. Moreover, they continue to hone, improve, and evolve those campaign plans through continuous probing and occasional limited attacks on our government and civilian infrastructure, networks, and systems. Doctrinally and otherwise, our adversaries are bent on shaping, influencing, deterring, and/or coercing USG decision-making, military freedom of action, and even public opinion in ways that will tend to shift the odds in their favor.

Mission Assurance Must be Part of Our Warfighting Doctrine.

The Nation's warfighters, and the entire DOD support establishment, must own this new reality in the assessment of MA risk as an integral part of operational planning. In many ways, it is easier or more beneficial for adversaries to target U.S. forces at home, either well before or at the beginning of a potential crisis. United States Transportation Command (USTRANSCOM), for example, is very dependent on civilian transportation infrastructure, systems, and cyber networks to augment the military's own capacity to support force projection. The Defense Logistics Agency (DLA) is likewise tied to civilian suppliers and their logistics supply chain. DLA is thus a high-priority target for any enemy determined to limit if not curtail the availability of the fuel and spare parts vital to the mobility and lethality of our energy-dependent and technologically advanced force. Operational plans (OPLANs) can no longer assume there will not be tangible threats to transportation or that the fuel our forces need "is always going to be there."

The Nation's adversaries are well aware of our possible vulnerabilities and the need to exploit those vulnerabilities to the fullest in any escalation of potential conflict. In many ways, that conflict has already begun. As the threat continues to change and accelerate, seemingly faster than we can respond, we are faced with a strategic dilemma in considering the future evolution of MA policy and practice. This dilemma centers on the need to make a key paradigm shift in how MA may be viewed by the operational warfighting community.

National Security Requires Use of Both Sword and Shield.

Having evolved largely out of the former Defense Critical Infrastructure Program (DCIP) and Joint Staff Integrated Vulnerability Assessment (JSIVA) regimes, MA policy attempts to move away from what has been a somewhat inward focus on the vulnerability of assets and installations to a broader consideration of risk to operational missions. Nonetheless, MA practice is still largely embedded in and viewed through the lens of either the installation & logistics (I&L) or physical security organizations of the service components versus line

operations. Moreover, even within joint organizations and agencies where MA may be the province of operations, the focus may still be too narrowly fixed on installation or asset vulnerability and not sufficiently on assessing and mitigating risks to warfighting missions.

Where warfighting capability is the Nation's sword, MA can be considered its essential shield. Effective defense of the Nation requires the coordinated application of both. DOD continues to improve its ability to identify mission essential functions, assess risks to those missions, manage mitigation, and monitor the buy-down of risks over time. Along the way, the strategic importance of MA to the protection of our warfighting capability is becoming better understood by an as-yet relatively small community of MA practitioners. That advance aside, MA is not yet fully reflected in warfighting doctrine or incorporated as an integral element of operational planning at the combatant command or service component level. It must be a larger part of our warfighting mindset and "the operators have to own it."

Planning Must Account for a Potentially Contested Homeland.

Though there are signs of positive change, the dynamics of current and future threats require a more fundamental shift in our thinking about how potential risks to operational missions need to be a greater priority for warfighting commanders. They simply cannot afford to be sanguine about the mission assurance of their own capabilities or that of the supporting establishments like USTRANSCOM and DLA. Likewise, those agencies must consider the implications of MA risks not only in the context of their own operations but in terms of how those are interdependent with the operational missions of the supported commands.

With the contemporary battlespace extending from the regional combatant commands (COCOMs) back to the homeland, warfighting abroad and homeland defense have become tremendously interdependent and the line of demarcation between the two far less distinct, especially in the cyber domain. Though some major commands are beginning to identify both defense and civilian-owned infrastructure security risks in the context of homeland defense, especially as those pertain to DOD MA, these issues may not be covered sufficiently in current OPLANs or what would otherwise constitute MA annexes to those OPLANs. With MA and homeland defense so intertwined, operational planning must account for a potentially contested homeland.

A New Civil-Military Partnership is Now Essential.

There is continuing improvement in the way key federal agencies like DOD, DHS, and the Department of Energy (DOE) are collaborating in a "whole-of-government" approach to the defense of the Nation's critical infrastructure. That includes understanding the national security and military implications of risks to the civilian infrastructure on which DOD relies.

However, government alone cannot predict and assess risks to civilian-owned infrastructure, systems, and networks nor can it alone effectively mitigate the risks tied to those things it does not own or control. A new partnership between the military, civilian government, and private sector industry is required in what must be a comprehensive "whole-of-nation" effort.

The private sector is a central player that must be involved in nearly every aspect of planning and coordination in the defense of the homeland, and even in the extension of that key involvement to the protection of U.S. defense interests abroad. The USG continues to partner where possible, but could benefit from even greater industry inclusion in exercises that are currently government-only. Government agencies at all levels – not just Federal – need to develop relationships with the private sector in the interest of homeland defense and security. In any "worst day" scenario, industry will be an indispensable element of incident response.

With the Right Engagement, Industry Will / Must Lean-In.

DOD has capabilities, policies, and plans for Defense Support of Civil Authorities (DSCA) in times of national emergency. But what about civilian support for Defense authorities in a national security crisis? What can lead civilian agencies and the private sector do, to better support the Defense effort and the protection of its own infrastructure? In the event of such a national crisis, and even before, DOD must clearly define its priority requirements for support from civilian industry. It must also "harshly prioritize" any of its own capabilities that might otherwise be diverted to the defense of infrastructure in the homeland given the potential all-out nature of future conflict. While some businesses in critical sectors may have incentives or financial concerns that do not necessarily align with this more mutual notion of support, the general sense from private sector partners is that "industry wants to lean in."

The answer to a more effective partnership, however, is not simply more "information sharing" but a more meaningful level of military-civilian engagement in understanding mission criticality, assessing associated risk to the infrastructure on which DOD depends, and highly coordinated yet parallel efforts to mitigate those risks in the overarching interest of national security and homeland defense. The potential consequences to the Nation are too great to do otherwise. Moreover, that partnership cannot just be reactive in nature. Industry and government "can't defend their way out of the problem." This is particularly true for cyberwarfare where there is a need to bring industry into the active cyber defense effort.

Strategic Infrastructures, Networks, and Systems are at Risk.

One challenge to partnership from an industry perspective, is working with a large number of government agencies making a multitude of differing and potentially competing demands. Fewer points of contact and a "harmonized" set of requirements would ease confusion and

decrease the costs and complexity of engagement. Approaching industry sector-by-sector, in partnership with DHS and other interagency partners, may be a way to make improvement. One such sector is logistics and the civil-military supply chain. Due to renewed threats to the homeland, traditional assumptions about the security of military logistics, and other strategic lifeline infrastructures, networks, and systems vital to national defense, must be questioned.

Until now, direct attacks on the homeland have been considered low probability/high consequence events due to the geographic protection of the oceans and conventional military superiority. The probability of asymmetric attacks, especially those below the threshold of armed conflict, has since increased significantly and the potential consequences remain similarly high or even higher. Not since World War II have our adversaries seriously challenged DOD's ability to deliver personnel, equipment, and supplies to the war zone. Our warfighters have come to expect and rely on the fact that what they need will be there. The return of great power near-peer competition again calls this assumption into question. Most of U.S. force projection capabilities are now CONUS-based. Attacks that hamper force mobilization can have major strategic effect. DOD needs to give greater consideration to the potential impacts of a disruption to Defense transportation and the logistics supply chain.

We Cannot Just Defend Our Way Out of the Problem.

The nation has too many targets to defend and not all are equally critical or vulnerable. Nor are all equally important to military operations or, for that matter, national resilience. However, even with careful prioritization, the protection of what is most vital may still be beyond the scope of even a "whole-of-nation" strategy. As a result, an effort is needed to mitigate potential risk by shaping the threat environment such that our adversaries are deterred from attacking critical infrastructure targets – especially civilian ones. There are three mutually supporting ways to achieve that deterrence:

- **Partner with Industry** – Implementing effective deterrence will require significant industry participation. DOD has some methods that contribute to collective deterrence, but it must work with industry to improve policies, procedures, and coordination.
- **Create the Right Incentives** – It is not up to DOD alone. The USG must incentivize industry participation as part of a national strategy. That strategy must also identify risks in the development stage and work to remediate them early and at lower cost.
- **Hunt for Archers, not Arrows** – As noted in the DOD Cyber Strategy, the USG must defend forward and be proactive in preempting the threat. Government will need industry to help find these 'archers,' bait them, and participate in their incapacitation.

Defense responses to asymmetric threats will differ based on the attacker. Note the contrast between Russia as a "descending, impatient" power and China as an "ascending, patient" one. Russia is developing extremely advanced capabilities, but not to scale. China is rapidly modernizing, but steadily to scale. Neither can win a conventional war against the U.S. alone, but both are attempting to close the gap in their own way. Russia has clear economic concerns, while China is worried about internal stability. Can the U.S. design offensive capabilities that threaten to exacerbate those challenges if provoked? Symmetric capabilities alone will not serve a deterrent function because our adversaries know we are unlikely to employ them in scenarios below a certain threshold. In response to potential asymmetric threats, the USG needs to advance preemptive deterrence capabilities, below the threshold of war -- capabilities which our enemies know exist and that we are sure to use in retaliation.

PANEL #2

MISSION ASSURANCE CIVIL/MILITARY INTERDEPENDENCIES

Speakers/Panelists
Vayl Oxford, Director, Defense Threat Reduction Agency, DOD
Randy Smith, Assistant Deputy Commandant (Security), PP&O, HQMC
Arthur Kitt, Director for Mission Assurance, J31, Defense Logistics Agency, DOD
Capt. Joe Coccia, USCG (Ret.), Port Security Manager, Port Authority of NY&NJ

Moderator
John Paczkowski

In his opening to the *2018 National Defense Strategy (NDS)*, the Secretary of Defense stated, *"In this environment, there can be no complacency – we must make difficult choices and prioritize what is most important to field a lethal, resilient, and rapidly adapting Joint Force." Lethal* represents the sword of our Nation's combat capability and *resilient* being the shield that preserves military capacity and enables the execution of Defense missions, or what we call mission assurance.

In describing the development of a more lethal, agile, and resilient joint force, the 2018 NDS outlines a Global Operating Model that constitutes four layers of joint force posture and employment – contact, blunt, surge, and homeland defense. This model is intended to facilitate the achievement of both DOD's competition and wartime missions that span the continuum of aggression in an increasingly asymmetric threat environment. In addition to modernizing and strengthening conventional capabilities, the model is designed to *"…help us compete more effectively below the level of armed conflict; delay, degrade, or deny adversary aggression; surge war-winning forces and manage conflict escalation; and defend the U.S. homeland."*

Stronger Civil-military Collaboration is the Next Leap Forward.

A decisive conventional force and strong nuclear deterrent keep our enemies from wanting to go to war and thus avoiding direct, armed conflict. So instead, they operate just below that level in the "grey zone," competing to not only achieve their military, political, and economic aims unmolested but to also gain whatever asymmetric advantage possible should hostilities escalate. The uniformed services are in a "full sprint" to improve readiness and modernize their conventional capabilities. However, aggression in the grey zone presents our greatest current challenge, not only in terms of overarching Defense strategy but in the more strategic assessment and mitigation of MA risk in this highly active threat environment.

Near-peer adversaries are making significant strides in grey zone capabilities. The evolution of the digital environment creates a nebulous boundary for the United States to defend. The wolf is no longer at the door but is now inside our boundary. China has been conducting an aggressive and extensive surveillance and data-gathering campaign. The Office of Personnel Management (OPM) breach and continued theft of military secrets and intellectual property (IP) – highlighted by China's copycat development of the J-31 stealth fighter – have received much attention. However, the proliferation of Chinese-manufactured Unmanned Aircraft Systems (UAS) that send data back to China is also raising concerns. China does not have the same challenges we face in terms of collaboration between government and industry, because the government of China has tight-fisted control over their private sector. Likewise, if we are in a renewed arms race with Russia, it was suggested that, "We don't even have our track shoes on yet." Assessing more global risks to the DIB and forging closer civil-military collaboration are increasingly important components to the next evolution of Defense MA policy.

Our Key Risks Lie in the Space Between Organizations and Systems.

The assets, networks, and systems that our adversaries are targeting do not necessarily lie neatly within a single command, agency, or organization's domain. The most attractive targets will tend to be those that transcend organizational boundaries and span multiple stakeholders. They are the potential weak points at the gaps and seams where ownership is shared, responsibility is vague, and where end-to-end risks may not be adequately identified, either due to an absence of a single whole-system view or clear accountability. Moreover, there also exist interdependencies between these assets where owners and operators may not be aware of the cascading effects of a disruption or loss and thus have different perceptions of vulnerability and risk than those stakeholders either upstream or downstream in the chain. This is further complicated by our interdependence with allied and host nation infrastructure.

As we respond to the challenge of hybrid and asymmetric threats in an evermore complex multi-domain battlespace, one that ranges in time across the continuum of competition-to-conflict, it will be increasingly important for us to consider MA in a whole-system context. Assets, networks, and systems that transcend organizational boundaries and singular ownership include what DHS refers to as lifeline infrastructures – energy, communications, transportation, and the logistics supply chain. Risks to these interdependent and highly networked infrastructures that do not reside within the purview of a single owner must be assessed both end-to-end at the system layer and within a regional context. The latter is focused on asset, network, and system interdependencies within the homeland or a particular area of responsibility (AOR). Though there is increasing attention to outside-the-wire (OTW) interdependencies, system-wide and theater-level approaches, tied to OPLANs, are needed.

We Need to Better Exploit What We Already Know.

The Defense Threat Reduction Agency (DTRA) conducts both Balanced Survivability Assessments (BSAs) and the Joint Mission Assurance Assessment Program (JMAAP). Both initiatives inform the risk management efforts of major joint and service commands and installations against a broad spectrum of threats. While BSAs key on the survivability and mission continuity of vital U.S. and allied national / theater-level assets, the JMAAP focuses on the protection, continued function, and resilience of Mission Essential Functions (MEFs) in compliance with overarching MA requirements. The JMAAP is complementary to and runs parallel with the MA programs of individual service components and DOD agencies.

DTRA MA assessments are performed on a recurring 3-year cycle, though the agency can conduct specific assessments out of cycle by request. As crosscutting issues emerge from the JMAAP, DTRA makes reports of those findings to the DOD MA Executive Steering Group for collective action. It has recently assumed stewardship of the Department-wide Mission

Assurance Risk Management System (MARMS) and intends to use the database in a more dynamic way – as an active system, rather than simply a static data repository. A significant amount of data on DOD vulnerabilities has been collected through the BSA, JMAAP, and service and agency-level MA programs. DTRA is now exploiting that data by conducting analysis to identify vulnerability trends of shared interest. Given the asymmetric nature of the threat and the target attractiveness of assets and systems that span individual commands and agencies, harmonizing data management across DOD is key to a more strategic and unified MA effort.

Hidden Risks are Embedded Upstream in the Chain of Interdependency.

As DOD works to assess risk to operational missions more comprehensively by addressing vulnerabilities to defense-owned assets and capabilities, there is also a need to help industry assess its own vulnerabilities that could have far-reaching consequences for MA. This goes beyond the risks associated with DOD dependence on civilian-owned critical infrastructure, networks, and systems that are outside the fence line. It also extends to the manufacture of equipment and spare parts further up the procurement supply chain. DLA and other DOD components depend heavily on civilian industry for the acquisition of mission essential fuel, warfighting supplies, and other commodities, in addition to sophisticated and increasingly interconnected weapon systems. Thus, especially problematic are challenges related to the cybersecurity environment in which Defense contractors and vendors operate.

Cybersecurity requirements for DOD prime contractors do not necessarily flow down to their immediate subcontractors. Nor might DOD even have direct line-of-sight on the second and third-tier vendors that supply critical subcomponents for Defense equipment and weapons systems, creating potential "built-in" vulnerabilities. DHS is facing a similar challenge in working with industry to protect the civilian manufacturing and logistics supply chain. In that context, it is also not uncommon for industry partners to have no visibility beyond the first or second node out in that chain. This is especially problematic if lower-tier suppliers are owned by adversarial entities. The bottom line is that DOD does not have a good handle on interdependent risks, especially cybersecurity risks, among its private sector contractors and vendors or the protection of their defense-related IP and other sensitive information. One small compromised component could bring down an entire DOD system. The challenge is even greater if the component is widely deployed across multiple mission essential systems.

Risk Assessment Must Take a Wider Whole-Systems View.

Industrial espionage by near-peer competitors to achieve economic parity is serious enough, but the close alliance between the military and industry of our top adversaries, and their joint efforts to position for an asymmetric military advantage, causes a whole new set of MA risks. For example, an adversary company or surrogate leases space in a building it owns to a U.S. defense

contractor. The building operates the Wi-Fi service and thus has visibility into the potentially defense-sensitive data and information flowing through that network. Chinese 5G network providers and chip manufacturing industries pose a similar but more universal threat to not only the U.S. and its allies but to the security of other nations across the globe. Both DOD and DHS must work more closely with industry to address this gap in MA security.

The *Mission Assurance Strategy of 2012* focuses on identifying risks to and strengthening the resilience of DOD MEFs to include the protection of end-to-end systems like information networks and the supply chain. Nonetheless, current MA guidance (DoDD 3020.40 and DoDI 3020.45) seems to place heavy emphasis on individual pieces of Defense Critical Infrastructure (DCI). It thus may be interpreted too narrowly toward an inward emphasis on an organization's own physical assets, creating challenges for agencies like DLA. That agency sits atop a highly interdependent, networked, and cyber-intensive military logistics system. That system has thousands of civilian suppliers on one end, scores of component and agency customers on the other, and DLA as the responsible enterprise in the middle. The agency does not own many hard assets and its mission responsibilities clearly go beyond the narrow scope of prioritized DCI. DOD must further clarify guidance concerning MA for crosscutting systems that transcend singular ownership and accountability, like the military supply chain.

Models for Better Civil-Military Engagement Already Exist.

Given the characteristics of an asymmetric threat, the nature of potential targets, and the need for more comprehensive engagement with the private sector, what are the existing models to which we can look? In the face of unprecedented threats, can we legislate new requirements for better collective security to both protect critical infrastructure at home and help assure the success of military missions abroad? The Security and Accountability for Every Port (SAFE Port) Act of 2006 may be one such example. Its enactment in the wake of 9/11 responded to national security concerns over possible transport of weapons of mass destruction (WMD) into the U.S. through maritime channels and serious questions about the sale of American port facilities to foreign-owned companies. The SAFE Port Act established a new security regime for port operators, mandated port worker vetting and credentialing, and initiated new partnerships with industry and the international port community for better maritime security.

As the lead agency for the security of port and maritime commerce, the U.S. Coast Guard is a positive example of well-established public-private partnerships (P3s) for homeland security between a federal agency and the transportation sector. Area Maritime Security Committees (AMSCs) provide collective stewardship of port security in a given Coast Guard sector. AMSCs are made up of a cross-section of public-private port interests and are chaired by private sector representatives. The Coast Guard depends on these industry partners to help assess risk, shape

mitigation priorities, and execute port security plans while ensuring their own implementation of mandated security regulations. Port facility operators are required to conduct vulnerability assessments, develop and update individual security plans, and are subject to 24/7 inspection by the Coast Guard to enforce compliance. AMSCs have served to significantly increase public-private transparency, information sharing, and collaboration.

Take a Balanced and Holistic Approach to Physical and Cyber Risk.

The Port of New York is the third largest port by volume in the U.S., with China as its top trading partner. While it is no longer considered a primary strategic port, DOD remains the primary shipper of various commodities from its facilities. As a further example of the value of AMSCs as a P3 initiative, the New York AMSC's cybersecurity subcommittee conducts industry-government cybersecurity exercises. Those exercises include organizations like Goldman Sachs, AT&T, ConocoPhillips, and Maersk – the world's largest shipping company. Through these exercises and otherwise, the private sector continues to express concerns over liability risk and financial exposure that may limit or dis-incentivize the disclosure of cyber-security vulnerabilities or breaches. DHS continues to engage industry on these issues and its new Cybersecurity and Infrastructure Security Agency (CISA) is a fresh opportunity for DOD to partner with DHS and engage industry in more robust cybersecurity discussions.

While cyber threats are likely among the most concerning, they remain just one critical factor among a broad array of risks to DOD missions. With the tremendous national emphasis on and sometimes stove-piped approach to cyber, DOD must be careful about developing a separate and too narrow focus in this domain. Since our adversaries' strategy will likely involve the combined application of asymmetric tactics, what is needed is a more integrated view of the most significant threats and the synergistic effect of the MA risks they present. The pursuit of a balanced and holistic approach to vulnerability assessments and portfolio-based risk management, that includes cyber as a key element, must continue. Closely associated with cyber as an MA concern is the insider threat. Each of the critical infrastructures, networks, and systems considered in MA assessments have an inherently human aspect that may at times be overlooked. While a focus on assets helps with risk management and prioritization, there must also be a greater MA effort applied to considering malicious actors inside the fence line.

Warfighters Must be a Driving Force for Change.

Finally, it is up to commanders at all levels to establish risk-based priorities, pursue the necessary resources, and take action when MA vulnerabilities are identified. Over the years, a tremendous amount of information on MA vulnerabilities has been amassed and there are indications that associated reports are sometimes not acted upon and "sit on the shelf." With the vital importance of MA to warfighting, it is essential that the challenges associated with MA risk

management and the implementation of risk mitigation be examined and corrective action pursued. Accordingly, consideration should be given to changing the mindset concerning MA as "compliance" requirement to one more aligned with warfighting and the resilience of combat capability – the sword and the shield. As a warfighting concern, changes in warfighting doctrine, our approach to operational planning, and the consideration of MA risk in operational decision-making are needed. Until the operational community fully embraces MA, risk mitigation may continue to struggle for leadership attention and resources.

PANEL #3

INDUSTRY/GOVERNMENT INTERCHANGE AND COLLABORATION

Speakers/Panelists
Bruce Walker, Assistant Secretary, Office of Electricity, DOE
Robert Kolasky, Director, National Risk Management Center, DHS
Scott Aaronson, Vice President, Security & Preparedness, Edison Electric Institute
Kathryn Condello, Sr. Director, National Security & Emergency Preparedness, CenturyLink

Moderator
Frank Cilluffo

Industry-government P3s focused on the protection of critical infrastructure and cyber networks are starting to produce important, tangible results. Going forward, the DOD, its federal partners, and the private sector need to build on this progress, and avoid reinventing the wheel. The Tri-sector Executive Working Group formed by DHS is one recent example of this progress. That group includes industry and government representatives from the Energy, Communications, and Financial Services sectors, working in partnership with the new DHS National Risk Management Center (NRMC) within CISA.

New Opportunities for Civil-Military Collaboration are Emerging.

As a homeland security-focused P3, the Tri-sector Executive Working Group facilitates an integrated and collaborative approach to the identification of common vulnerabilities and risk management through joint prioritization, planning, and response to catastrophic events. It also helps direct intelligence requirements and is building cross-sector risk management playbooks. The Working Group has helped with drafting the forthcoming revised National Response Framework, and the creation of Emergency Support Function (ESF) #14 for cross-sector response operations. It is just now leaning forward in the development of a cybersecurity playbook. Industry-only coordination also takes place within the Working Group (and indeed predates coordination with DHS). The Tri-sector Executive Working Group complements existing industry Sector Coordinating Councils (SCCs) established under the NIPP and Information Sharing and Analysis Centers (ISACs) that predate the establishment of DHS.

For its part, DOE, to include its National Nuclear Security Administration (NNSA), is making progress in working collaboratively with DOD to identify Defense Critical Electric Infrastructure (DCEI). The identification of DCEI is a requirement under the Fixing America's Surface Transportation (FAST) Act. DOE and DOD, under a joint DCEI Task Force, have distilled a list of critical electric infrastructure assets down to less than 100 locations across the two departments, though there is still more work to do to identify DCEI nationwide. The goal is to pinpoint the top 10% most important assets for continuity of government and to help DOD better mitigate MA risk due to a loss of commercial power.

DOE is also working with DHS and the Coast Guard to identify key maritime ports, and then collaborate with relevant public and private sector partners to facilitate investments in security and resilience. Steady progress is being made, including a technical conference on incentive-based rates to motivate utilities to make investments in risk mitigation for port protection and continuity of operations. DOE is likewise engaged with the Department of Housing and Urban Development (HUD) on the accessibility of funds for Investor-Owned Utilities (IOUs) and P3s. HUD recently made a key policy change to open up billions of dollars in Community Development Block Grant (CDBG) mitigation funding to utilities.

CISA is a Key Focal Point for Government-Industry Collaboration.

The DHS NRMC was recently formed with the idea that "it's time to get serious about strategic risks to the nation's infrastructure." The center is the focal point for coordinated planning, analysis, and collaboration to identify and address the most significant risks. It is a unified effort between industry and government that fosters joint work within and across industry sectors. The Center interfaces with SCCs to bring industry more directly into key national security conversations and champions P3 initiatives like the Tri-sector Executive Working Group. There used to be a bigger gap between homeland defense and homeland security. That gap has now eroded. For all the reasons stated earlier, DHS and DOD are now facing the same problem set with a higher level of interdependence than ever before. Thus, collaboration between the two, plus other federal partners, and industry is growing but needs to accelerate if we are to match the pace of this looming asymmetric threat.

NRMC has re-organized its risk management approach to focus on the potential impacts and consequences of attacks on critical infrastructure, and is using that to inform related sector dependency analyses and risk prioritization efforts. This outcome-based planning also brings industry to the table early, and not as an afterthought. Cyber threats are clearly a key risk factor. NRMC's critical infrastructure resilience strategy recognizes that adversaries are trying to achieve strategic effects by holding U.S. infrastructure owners and operators (and those of our allies) hostage under the potential threat of cyber-enabled attack. As a result, the U.S. needs to think more strategically about risk mitigation beyond physical and cybersecurity hardening efforts. National risk mitigation must increasingly emphasize deterrence.

NRMC is a shift from a largely reactive P3 framework that consisted mostly of information sharing to more proactive engagement in which industry and government increasingly work together to identify, assess, prioritize, and reduce risk. The shared-ownership model reflected in the Tri-sector Executive Working Group will be expanded to other infrastructure sectors.

The NRMC has two main "buckets" of activity:

- **Cross-sector Analysis** – This analysis helps industry and government understand threats and consequences, determine the criticality of assets as part of the overall prioritization effort, and explore cross-sector interdependencies. NRMC then examines the down-stream and cascading consequences of disruption for the highest priority infrastructure.
- **Infrastructure Protection Initiatives** – NRMC is working on creating repeatable processes to reduce risks to critical infrastructure. To date, these initiatives include an Information Communications Technology Supply Chain Task Force and a cooperative effort between DOE and the Transportation Security Administration on pipeline security.

Increasing Emphasis is to be Placed on Interdependency.

In addition to racking and stacking top-level risks to lifeline infrastructure sectors, NRMC is looking at shared vulnerabilities to cross-cutting industrial control systems, and key inter-dependencies between sectors that threaten to impose mutually-reinforcing failures. DHS partnerships in this space should be considered along two axes: North-South, between industry and government; and East-West, between different critical infrastructure sectors.
The creation of ESF #14 within the newly revised National Response Framework will also further support collaborative cross-sector risk assessment, planning and operations.

Since DOD is a customer for many lifeline sectors, those industries generally recognize their role in national security and generally want to support Defense MA. As evidence, note the considerable work being done by DHS to further energize P3 relationships for homeland security. Industry is already leaning in and coming to better understand the military notion of supporting versus supported commands in the context of its role in national security and MA. However, strategic partnerships of this kind must work both ways. Government needs to work with industry to create an environment conducive to collaboration and address its concerns about liability and the protection of sensitive proprietary information.

There are Lessons to be Learned from the Communications Sector.

The communications sector has a number of legacy mechanisms for industry-government engagement, which were initially formed by the Defense Department to support continuity of operations/continuity of government (COOP/COG) and by extension what we are now calling MA. The imperative to preserve National Security and Emergency Preparedness (NS/EP) communications and support COOP/COG in times of national crisis is built into the genetic fiber of the communications sector. The industry already provides extensive support to government via the President's National Security Telecommunications Advisory Committee (NSTAC), including the Network Security Information Exchanges (NSIEs).

Industry-wide information sharing, including intelligence and the management of sensitive information, is improving. The communications and financial services sectors are increasingly "leaning forward" and trying to drive intelligence requirements. The USG Intelligence Community (IC) has also gotten better at providing information, including that which comes through the National Cybersecurity and Communications Integration Center. The delta between 'first to know' and 'last to know' within industry has compressed greatly. One challenge for P3 coordination is "language." Industry and government agencies have different terminology for similar concepts. It works both ways. Industry has to work within government frameworks but the public sector has to keep up with industry developments.

That lack of clarity in terminology and concepts at times makes it harder for either set of stakeholders to articulate particular issues, potential solutions, and areas for mutually beneficial coordination. Another major challenge for industry-government coordination is the co-mingling of industry and government resources. Joint efforts have faced legal and normative challenges (i.e. "It hasn't been done that way in the past."). How can industry and government work to close that gap? There is still considerable policy work to be done to allow for more joint investment. This also includes the transfer of technology. DOD and the broader USG have a vested interest in ensuring the resilience of privately-owned critical infrastructure. How can government get technology and capabilities that enhance industry resilience and thus support mission assurance into the hands of commercial industry?

Both National Policy and Funding Will be Needed.

To address MA risks, industry and government need both policy and capital. "Policy without money is irrelevant; but money without policy guidance is also problematic." How can government and industry find more money to address MA risk mitigation needs? The answer is "it depends." Regulatory incentives are one way. The Office of Management and Budget (OMB) has been a problem. Despite identifying DOD systems that need protection, and proposing a plan to do so, there are perceptions that OMB has declined the requested funds. In some cases, utilities are going forward themselves. Some industry leaders are willing to lean in a bit and take risks – but not on a level that will scale sufficiently to address the problem. Small companies often have less resources to proactively engage in this area. Clearly the answer to addressing mission assurance related to civilian-military interdependencies goes beyond the risk management efforts of either party alone. It must include a more robust and coordinated effort to address the policy and funding issues that may inhibit meaningful improvement.

CLOSING DISCUSSION

Speakers/Panelists
Charles Kosak, Deputy Assistant Secretary of Defense, DC&MA

Moderator
Frank Cilluffo

The major takeaway from this Policy Forum is that, despite important progress, the U.S. is still behind the curve in addressing risks from emerging threats to MA and needs to accelerate progress in the future or that gap will only widen. Mission Assurance is more important than it has ever been. Attacks on the homeland are no longer hypothetical "high impact, low frequency" events. Aggressive activities by our adversaries, just below the threshold of conventional conflict, are "game changers" for the military. We need to think strategically, within DOD and with industry, about how to address these challenges going forward.

We also need to prepare for the threat of a hybrid / combined arms approach – simultaneous cyber, kinetic, and information attacks designed to achieve our adversaries' political and strategic goals – that may accompany regional conflicts. Since our adversaries' strategy will likely involve the coordinated application of asymmetric tactics, our MA assessments can no longer afford to consider the impact of a single risk scenario at a time in isolation of the possible cascading and reinforcing effects of others. Industry and government will need continuous intelligence assessments for these sorts of threats, with the IC, law enforcement community, and critical infrastructure owners and operators all on the same page.

Mitigating Asymmetric Threats is a Team Sport.

There is a need to leverage creative leadership and innovation if we are to better anticipate and get ahead of the hybrid and asymmetric attack profile of our adversaries – their tactics, techniques, and procedures (TTPs) – for operations below the threshold of war and beyond. Addressing these strategic challenges and mitigating the MA risk of various hybrid and asymmetric threat scenarios is a "team sport." It is bigger than any single government department or agency, or any one sector. It needs a "whole-of-nation" approach.

Our adversaries understand the complexity of these challenges and are looking to exploit vulnerabilities in the gaps and seams in our defenses – the places where perhaps we are less coordinated and responsibility is shared. Those adversaries may not attack Defense assets directly, but target single points of failure elsewhere. They will seek to cause cascading failures across multiple interdependent sectors with significant downstream consequences that threaten MA, public safety, the economy, and national security more broadly.

Bolstering national resilience against threats to MA will require ruthless prioritization, targeted investment, and close partnerships between industry and government, and across key industry sectors. All relevant stakeholders will need well-defined roles and responsibilities, and must take mutually-agreeable and specific actions to help mitigate collective risk. The "supporting versus supported" roles may be, at times, interchangeable. The 2018 NDS establishes a firm policy

foundation for many important initiatives. DOD and its industry and government partners need to work together and think creatively about how to operationalize those concepts in the interest of more robust MA and homeland defense.

A Great Deal Has Been Accomplished but Much More Remains.

Fortunately a great deal has been accomplished and there are new lessons learned regarding more effective approaches to meaningful industry-government collaboration. DOD and DHS also have much to learn from each other and, as stated before, the once wide gap between homeland defense and homeland security has all but been erased. We need to share what we know and build on what we have already done, while developing compatible and repeatable processes for assessing risk, managing mitigation, and monitoring improvement. We must do this together if we are to build stronger national resilience against the storm already brewing.

Investment to counter emerging threats will be needed but there must also be a clear and compelling "business case" for return on that investment in the buy-down of risk. DOD and its industry and government partners need to get to a place where they are collectively making "convincing" investments – not just implementing small, ad hoc projects at the margins. It is unlikely that our Nation will be able to defend against every attack and since we simply cannot mitigate all risk, we will also need to create response playbooks; so if and when the time comes, all stakeholders can and will take immediate and coordinated action.

Mitigation is Not Enough, We Also Need Meaningful Deterrence.

Beyond investments in risk mitigation and response preparedness, the USG needs to develop offensive capabilities, below the threshold of war, to improve the Nation's deterrence posture. We need campaign plans that are every bit as sophisticated and asymmetric as those of our adversaries. They must understand that the U.S. has both the capability and political will to take punitive offensive action if provoked and thus deny them the ability to achieve their aims and prevent them from making miscalculations that could precipitate an all-out conflict.

MODERATOR BIOGRAPHIES

Frank Cilluffo
Director, McCrary Institute for Cyber and Critical Infrastructure Security
Auburn University

Frank Cilluffo is the director of Auburn University's McCrary Institute for Cyber and Critical Infrastructure Security, and the Center for Cyber and Homeland Security. He serves on the Department of Homeland Security's Homeland Security Advisory Council, and was recently appointed by Congress to the Cyberspace Solarium Commission. Mr. Cilluffo is routinely called upon to advise senior officials in the executive branch, U.S. Armed Services, and state and local governments on an array of matters related to national and homeland security strategy and policy. Following the September 11, 2001 terrorist attacks, Mr. Cilluffo was appointed by President George W. Bush to the newly created Office of Homeland Security. There, he was involved in a wide range of homeland security and counterterrorism strategies and policy initiatives, and served as a principal advisor to Director Tom Ridge, directing the President's Homeland Security Advisory Council. Prior to his White House appointment, Mr. Cilluffo spent eight years in senior policy positions with the Center for Strategic and International Studies, a Washington-based think tank. There, he chaired or directed numerous committees and task forces on homeland defense, counter-terrorism and transnational organized crime, as well as information warfare and information assurance.

Dr. Paul Stockton
Executive Advisor, Center for Cyber and Homeland Security, Auburn University
Managing Director, Sonecon LLC

Paul Stockton is an internationally-recognized leader in infrastructure resilience, continuity planning, installation and personnel security, and U.S. national security and foreign policy. Prior to joining Sonecon, he was the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs from June 2009 until January 2013. In that position, he served as the DOD's Domestic Crisis Manager, helping lead the Department's response to Superstorm Sandy, Deepwater Horizon, and other disasters. Dr. Stockton also oversaw antiterrorism policies and programs for DOD's domestic installations, guided the Defense Critical Infrastructure Protection program and led the development of the DOD's first Mission Assurance Strategy. He was also responsible for DOD programs to strengthen security in the Western Hemisphere partner nations, leading DOD's talks on Defense Cooperation Agreements with Peru, Brazil and other key countries as well as defense policy coordination with Mexico and with Canada. In September 2014, Secretary of Defense Chuck Hagel named Dr. Stockton co-chair of the Independent Review of the Washington Navy Yard Shootings, which recommended major changes to DOD's security clearance system.

John Paczkowski
Executive Advisor, Center for Cyber and Homeland Security, Auburn University
Senior Vice President, ICF

A Senior Vice President at ICF, John Paczkowski leads homeland security and national resilience initiatives serving a range of government clients in the emergency management, infrastructure resilience, and defense mission assurance domains. A former executive at the Port Authority of New York and New Jersey, he led the agency's emergency operations center following the September 11, 2001, attacks on its World Trade Center complex. Thereafter, he directed its emergency preparedness, business continuity, and security efforts and was the architect of a 5-year $1.0 billion risk-based infrastructure security program. Mr. Paczkowski is a Fellow of the National Academy of Public Administration and serves as an Executive Advisor to the Auburn University's Center for Cyber and Homeland Security. He is a former Board Director for The Infrastructure Security Partnership and former Chairman of the Security Analysis and Risk Management Association. After 32 years of active and reserve service as a Marine Corps engineer and infantry officer, Mr. Paczkowski retired as a Colonel in 2005, his final tours include various homeland defense roles, among them Chief of the Civil Support Branch, Joint Operations Directorate, at the National Guard Bureau. He holds a B.S. in Industrial Engineering and an M.S. in Engineering Management from the New Jersey Institute of Technology, an M.A. in Organizational Psychology from Columbia University, and an M.A. in Security Studies from the Naval Postgraduate School.

PARTICIPANT BIOGRAPHIES

Kenneth Rapuano
Assistant Secretary of Defense, Homeland Defense and Global Security
U.S. Department of Defense

Kenneth Rapuano is the Assistant Secretary of Defense for Homeland Defense and Global Security. Previously Mr. Rapuano was a Senior Vice President at the ANSER Corporation, and Director of the Studies and Analysis Group which provided multi-disciplinary studies and operational analysis for a broad array of government clients in the national security and homeland security areas. Up until November of 2016, Mr. Rapuano directed the Homeland Security Studies and Analysis Institute, a Federally Funded Research and Development Corporation operated by ANSER. Mr. Rapuano served at the White House as Deputy Homeland Security Advisor to President George W. Bush from 2004-2006. He left the White House in 2006 to volunteer for deployment to Afghanistan with a Joint Special Operations Task Force, establishing and directing a targeting fusion center tracking high-value terrorists and insurgents. Mr. Rapuano served in Iraq in 2003, commanding the Joint Interrogations and Debriefing Center of the Iraq Survey Group established to survey and exploit possible weapons of mass destruction. He previously served in various senior positions including Deputy Undersecretary for Counter Terrorism at the Department of Energy, National Security Advisor to the Secretary of Energy and Special Assistant to the Assistant Secretary of Defense, International Security Policy. He served 21 years on active duty and in the reserves as a Marine Corps infantry officer and intelligence officer.

Charles Kosak
Deputy Assistant Secretary of Defense, Defense Continuity and Mission Assurance
U.S. Department of Defense

As the Deputy Assistant Secretary of Defense for Defense Continuity and Mission Assurance, he oversees the Department's continuity, mission assurance, domestic counter-terrorism, information-sharing and global anti-terrorism policies and programs. Prior to assuming his current position, Mr. Kosak served in OUSDP as the Principal Director for Strategy, Force Planning, and Mission Assurance, Principal Director for Partnership Strategy, Principal Director for African Affairs, Deputy Director for NATO Policy, and Senior Policy Analyst on the Balkans Task Force. Mr. Kosak also served as the Political Advisor to the Commanding General of V Corps, United States Army Europe which included deployments to Bosnia, Kosovo, Macedonia, Albania, and Israel. Prior to joining the Department of Defense, Mr. Kosak served as Head of Office for the International Rescue Committee (U.S. NGO) in Mostar, Bosnia and as a Program Officer in Tuzla, Bosnia. He also served as a Peace Corps Volunteer in the Congo.

Lieutenant General Reynold Hoover (Ret.)
Former Deputy Commander, U.S. Northern Command
Consultant, R N Hoover Consulting LLC

Lieutenant General Reynold Hoover is the former Deputy Commander, U.S. Northern Command, and Vice Commander, U.S. Element, North American Aerospace Defense Command. As Deputy Commander, General Hoover assisted the Combatant Commander in anticipating, preparing for, and responding to threats against North America and within Northern Command's assigned area of responsibility. Additionally, he provided oversight of Defense Support to Civil Authorities. General Hoover deployed in support of Operation Enduring Freedom from 2009-2010 where he commanded the Joint Sustainment Command in Kandahar and commanded the 167th Theater Sustainment Command from 2011-2014. From 2002-2003, General Hoover served as Chief of Staff for the Federal Emergency Management Agency (FEMA) and subsequently, he led FEMA's Office of National Security Coordination from 2003-2005. In 2005, General Hoover was appointed as Special Assistant to the President for Homeland Security and served as the Senior Director for Nuclear Defense and Continuity Policy on the Homeland Security Council. From 2014- 2016, he was the National Guard Bureau's Director of Intelligence and Director of Command, Control, Communications and Computers. Prior to his role at USNORTHCOM, General Hoover served as Mobilization Assistant to the Director of the Defense Intelligence Agency.

Major General Joseph Whitlock
Director, Army Protection
Headquarters Department of the Army

As Director, Army Protection Directorate, Major General Whitlock is responsible for strategic policy, planning, and coordination for: critical infrastructure, emergency management, protection assessment and policy, and insider threat and mitigation. He has served in several strategic plans and policy assignments, including Plans Officer in Third Army/ARCENT/Coalition Forces Land Component Command, Fort McPherson, GA and Operation IRAQI FREEDOM; Strategic Planner in the Office of the Assistants to the Chairman, Joint Chiefs of Staff for National Guard and Reserve Matters; Politico-Military Planner and Branch Chief, Strategic Plans and Policy (J5), Joint Staff; and Deputy Commander of Joint Base McGuire-Dix-Lakehurst, NJ. His general officer assignments include: Deputy Director for Strategy, Policy and Plans (J5), NORAD/ USNORTHCOM; Mobilization Assistant, Strategic Planning and Policy (J5), USPACOM; and his most recent assignment as Deputy Director for Politico-Military Affairs (Western Hemisphere), Strategic Plans and Policy Directorate, Joint Staff. He holds a Bachelor of Science degree from the U.S. Military Academy, a Master of Science degree in Operations Research from the Naval Postgraduate School, and a Master of Military Arts and Science degree in Theater Operations from the Command and General Staff College.

Dr. Richard Andres
Professor, U.S. National War College
National Defense University

Richard Andres is Full Professor of National Security Strategy at the U.S. National War College where he teaches courses on strategy development and cyber strategy and policy. Across his career he has served as a personal consultant on strategy to the Director of the National Security Agency-U.S. Cyber Command; the Secretary of the Air Force; the Commandant of the Marine Corps, and other national leaders. He has led strategy development teams for the Bush and Obama White Houses, various combatant commands and other government and private sector organizations. Dr. Andres teaches courses on cyber strategy at Georgetown University SSP and Johns Hopkins SAIS. He is a senior fellow at the Auburn University Center for Cyber and Homeland Security and sits on boards at the American Enterprise Institute and Pacific Northwest National Laboratory.

Vayl Oxford
Director, Defense Threat Reduction Agency
U.S. Department of Defense

Vayl Oxford, is the Director of the Defense Threat Reduction Agency (DTRA) located on Fort Belvoir, Virginia. Before being named DTRA Director, he was the National Security Executive Policy Advisor at the Department of Energy's Pacific Northwest National Laboratory (PNNL) where he was responsible for guiding the strategic direction and vision for national security issues. He served in multiple positions in the Department of Homeland Security (DHS) from 2003 to 2009, as the Policy Advisor to the Under Secretary of Science & Technology, as Acting Director of the Homeland Security Advanced Research Projects Agency, and as the first Director of the Domestic Nuclear Detection Office (DNDO), which was created to be the single entity in the U.S. government to protect the nation against nuclear terrorism. Appointed by President George W. Bush and reporting to the DHS Secretary, he led the development of the National Strategy to Combat Nuclear Terrorism. Prior to his appointment to DHS, Mr. Oxford served as the Director for Counter-proliferation at the National Security Council, where he supported the development of the President's National Strategy to Combat WMD, the policy and strategy for WMD interdiction, and represented the NSC in the development of the National Biodefense Strategy. From 1987 to 2002, he held several positions with DTRA and its legacy organizations (Defense Special Weapons Agency and Defense Nuclear Agency).

Randy Smith
Assistant Deputy Commandant (Security)
Plans, Policies and Operations, Headquarters U.S. Marine Corps

As Assistant Deputy Commandant, Mr. Smith is responsible for providing direction, supervising development, articulating emerging concepts, and advocating Marine Corps policies and capabilities for all issues pertaining to: mission assurance, anti-terrorism and force protection, law enforcement, Marine Corps security forces, Marine security guards, homeland defense, critical infrastructure assurance, physical security, counterdrug support, all CBRN related issues, and military support to civil authorities. He served over 25 years as a military police officer and during that time he held a variety of command and law enforcement staff positions to include MP company commander, provost marshal, H&S battalion operations officer, security officer for the Presidential Helicopter Squadron (HMX-1) and battalion commanding officer. Since being assigned to Headquarters Marine Corps, Mr. Smith served within the operations division as head, Security and Law Enforcement Branch. After retiring, he served as the Head, Mission Assurance Branch within the Security Division. He holds a bachelor of arts degree in Criminology from California State University and a master's of science degree in national security and strategic studies from The Naval War College.

Arthur Kitt
Director for Mission Assurance
Defense Logistics Agency

Arthur Kitt currently serves as the Defense Logistics Agency (DLA) Mission Assurance Program Director, Logistics Operations and Sustainment (J31). There he is responsible for the development and continuous improvement of policies, procedures, and technical aspects for the efficient operations of the DLA Continuity of Operations (COOP), Defense Logistics Sector and Agency Defense Critical Infrastructure (DCI) across the DLA Enterprise. He previously served as the senior DLA COOP and disaster planner, and oversaw all DLA COOP planning activities. Prior to DLA, Mr. Kitt was the Director of Contingency Planning for the Defense Finance and Accounting Service (DFAS). He was responsible for the development, implementation, and execution of a comprehensive DFAS-wide COOP, Disaster Recovery, Crisis Management Program and Emergency Operations Centers. Mr. Kitt held several prior positions, including Chief, Manpower Management/Deputy Resource Integrator for DFAS, DFAS Deputy Resource Integrator, and Manpower and Force Structure Analyst and Subject Matter Expert, 425th Transportation Brigade, U.S. Army Reserves. He retired a Colonel in the United States Army, serving seven years active duty and 23 years in the Army Reserves. Mr. Kitt has a BS Degree from Tuskegee University, a MS in Business Management from Webster University, and a MS in Strategic Studies from the United States Army War College.

Captain Joe Coccia, USCG (Ret.)
Port Security Manager
Port Authority of New York & New Jersey

Joe Coccia was appointed the Port Security Manager for the Port Authority of NY & NJ after joining the bi-state agency in 2014. He is a member of U.S. Coast Guard Sector New York's Area Maritime Security Committee (AMSC) Executive Steering Committee and also a member of the AMSC Cyber Security Subcommittee. Mr. Coccia is a retired U.S. Coast Guard Captain and former Captain of the Port (COTP) and Group Commander, Group/ Marine Safety Office for Long Island Sound in New Haven, Connecticut (2001 – 2004). Upon retiring from the Coast Guard, he was selected by APM Terminals North America (Maersk Lines) to be their first Chief Security Officer and later VP for Corporate Security & Compliance (Maritime) from 2004 - 2008. He has international consulting experience working for Richard A. Clarke's Good Harbor Consulting LLC. At that firm he was a senior foreign government maritime strategy and security consultant and project manager developing and implementing maritime strategy for the Emirate of Abu Dhabi, UAE. In 2010, he served as a critical incident management and pollution response expert while an operations consultant for BP on the Deepwater Horizon oil spill in the Gulf of Mexico.

Bruce Walker
Assistant Secretary, Office of Electricity
U.S. Department of Energy

Mr. Bruce Walker was nominated by President Donald J. Trump and confirmed by the Senate as Assistant Secretary for the Office of Electricity (OE) at the U.S. Department of Energy (DOE) in October 2017. The focus of his responsibility is to provide leadership on a national level to develop technologies to enhance the security and reliability of energy infrastructure and facilitate the federal and state electricity policy planning that shapes electricity and market operations. This is critical to meeting the Nation's growing demand for resilient electricity by overcoming the challenges of our Nation's aging electricity transmission and distribution system and addressing the vulnerabilities in our energy supply chain. Mr. Walker holds a Bachelor of Electrical Engineering from Manhattan College and a Juris Doctor in Law from Pace University where he was the technical editor on the Environmental Law Review and received an Environmental Law Certificate. He has completed the Distribution Systems program from Siemens, Power Technologies International. He is a distinguished graduate of the U.S. Air Force Academy Preparatory School and received an Honorable Discharge from the U.S. Military Academy.

Robert Kolasky
Director, National Risk Management Center, Cyber and Infrastructure Security Agency
U.S. Department of Homeland Security

Bob Kolasky was selected to lead the National Risk Management Center (NRMC) in 2018. As Director, he oversees the Center's efforts to facilitate a strategic, cross-sector risk management approach to cyber and physical threats to critical infrastructure. He most recently served as the Deputy Assistant Secretary and Acting Assistant Secretary for NPPD's Office of Infrastructure Protection (IP), before it became the CISA Infrastructure Security Division on November 16, 2018, where he led the coordinated national effort to reduce the risk posed by acts of terrorism and other cyber or physical threats to the nation's critical infrastructure. Mr. Kolasky has served in a number of senior leadership roles, including acting Deputy Undersecretary for NPPD before it became CISA, Director of Strategy and Policy for the Infrastructure Security Division, and Director of the DHS Cyber-Physical Critical Infrastructure Integrated Task Force to implement Presidential Policy Directive 21 on Critical Infrastructure Security and Resilience. He is also a former Assistant Director for the Office of Risk Management Analysis at DHS. Prior to joining DHS, he was a journalist and an entrepreneur. He helped start two of the first public policy web sites and served as the Managing Editor for IntellectualCapital.com.

Scott Aaronson
Vice President of Security and Preparedness
Edison Electric Institute

Scott Aaronson is Vice President, Security and Preparedness for the Edison Electric Institute (EEI). He joined EEI in 2009 in the government relations department focusing on security and technology issues, and most recently served as Executive Director of security and business continuity. He leads the EEI teams focused on cyber and physical security, storm response and recovery, and associated regulatory policy. In addition to his role at EEI, Mr. Aaronson also serves as the Secretary for the Electricity Subsector Coordinating Council (ESCC). The ESCC serves as the primary liaison between senior government officials and industry leaders representing all segments of the electric power sector. This partnership is held up as a model for how critical infrastructure sectors can work with government, yielding dramatic improvements in security and preparedness for the industry and the nation. Prior to joining EEI, he was a senior adviser to Members of Congress serving the 12th Congressional District of California, including former House Foreign Affairs Committee Chairman Tom Lantos. From 2001 to 2007, he served as an economic policy adviser to U.S. Senator Bill Nelson.

Kathryn Condello
Senior Director, National Security and Emergency Preparedness
CenturyLink

Kathryn Condello represents CenturyLink at the federal-level in all policy, planning and operational issues related to national security, emergency preparedness, disaster response, critical infrastructure protection, resiliency planning and continuity of operations. Ms. Condello is an operations-focused leader within CenturyLink and the Communications Sector, with extensive, executive-level experience in managing and directing broad corporate and industry initiatives in the areas of strategic planning, policy development, government relations, network deployment, operations and resiliency. Ms. Condello has more than 15 years of experience in industry initiatives associated with national security, network reliability, and emergency preparedness, planning and policy. She holds a B.A. from the University of Virginia, an M.B.A. from Loyola College, and served as a Principal Associate (Research Professor) with George Mason University's Critical Infrastructure Protection Program. Ms. Condello started her career in public safety radio, was one of the first commercial wireless pioneers, and gathered more than 20 years commercial wireless experience prior to joining CenturyLink. In 2001, Ms. Condello was named by Wireless Week as one of the 25 Influential Women in Wireless for her work on wireless priority service. Ms. Condello also served as Chair of the Communications Sector Coordinating Council, Chair of DHS NCC/Comms-ISAC, and CenturyLink Liaison to the National Coordinating Center.

AUBURN

UNIVERSITY

CENTER FOR CYBER
AND HOMELAND SECURITY

cchs.auburn.edu