13TH

HOMELAND SECURITY WEEK

October 22-24, 2018
College Park Marriott, Hyattsville, MD

CRITICAL FACETS IN PROTECTING THE HOMELAND

Volume III

FIND OUT MORE

www.HomelandSecurityWeek.com

13TH
HOMELAND
SECURITY WEEK

October 22-24, 2017 | Washington D.C.

Content Overview

Ensuring homeland security is a moving target—an on-going and eternally evolving battle. The latest technological changes, as well as the socio-political environment, both at home and abroad, contribute to the difficulty of the task.

In advance of **Homeland Security Week,** we've made it our mission to inform you of the latest innovations to facilitate the maintenance of a current and complete big picture view, so that you can more effectively do your duty.

INTELLIGENCE ANALYTICS

DIRECTED ENERGY

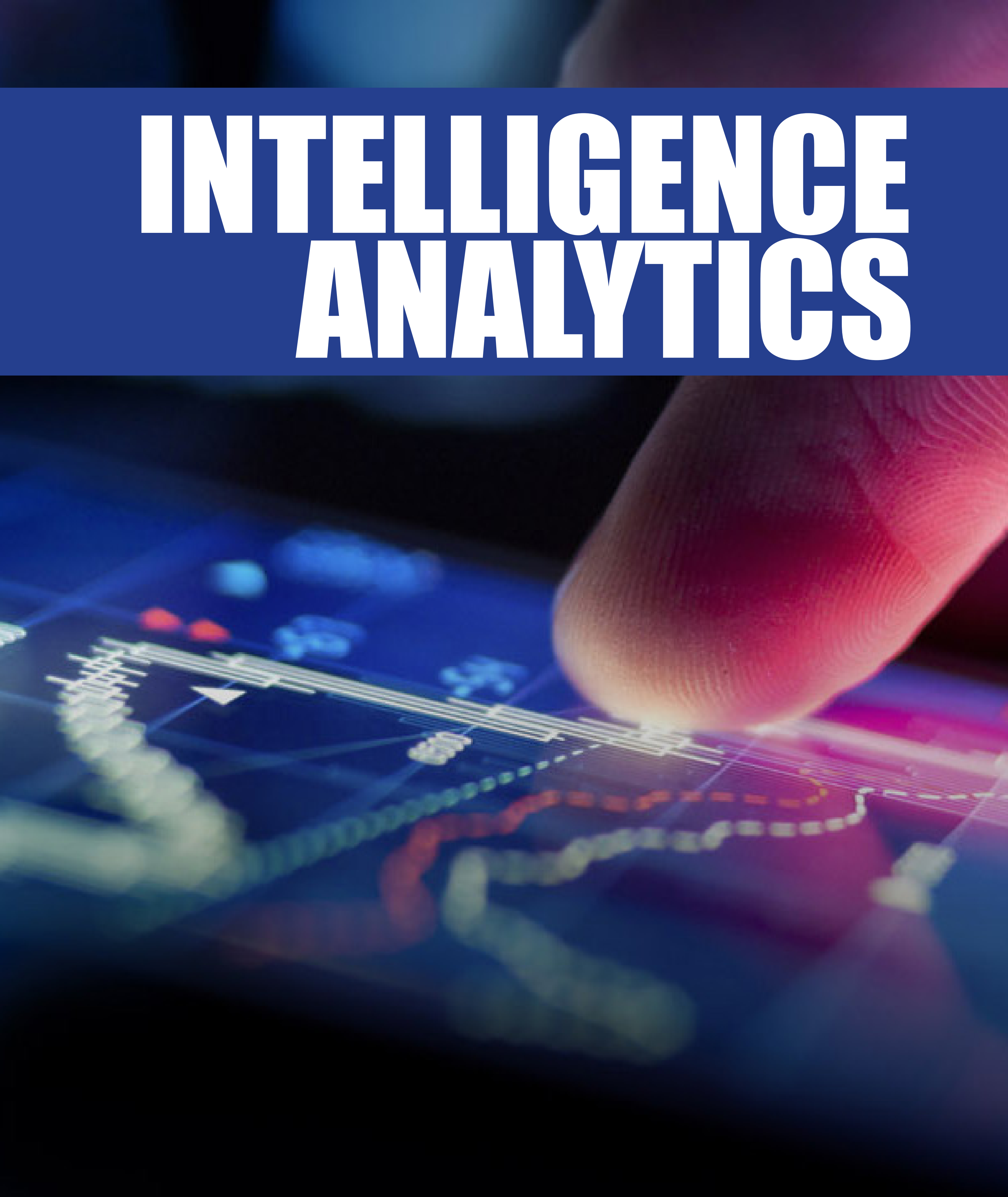
CRITICAL INFRASTRUCTURE

BIOMETRICS

CYBER SECURITY

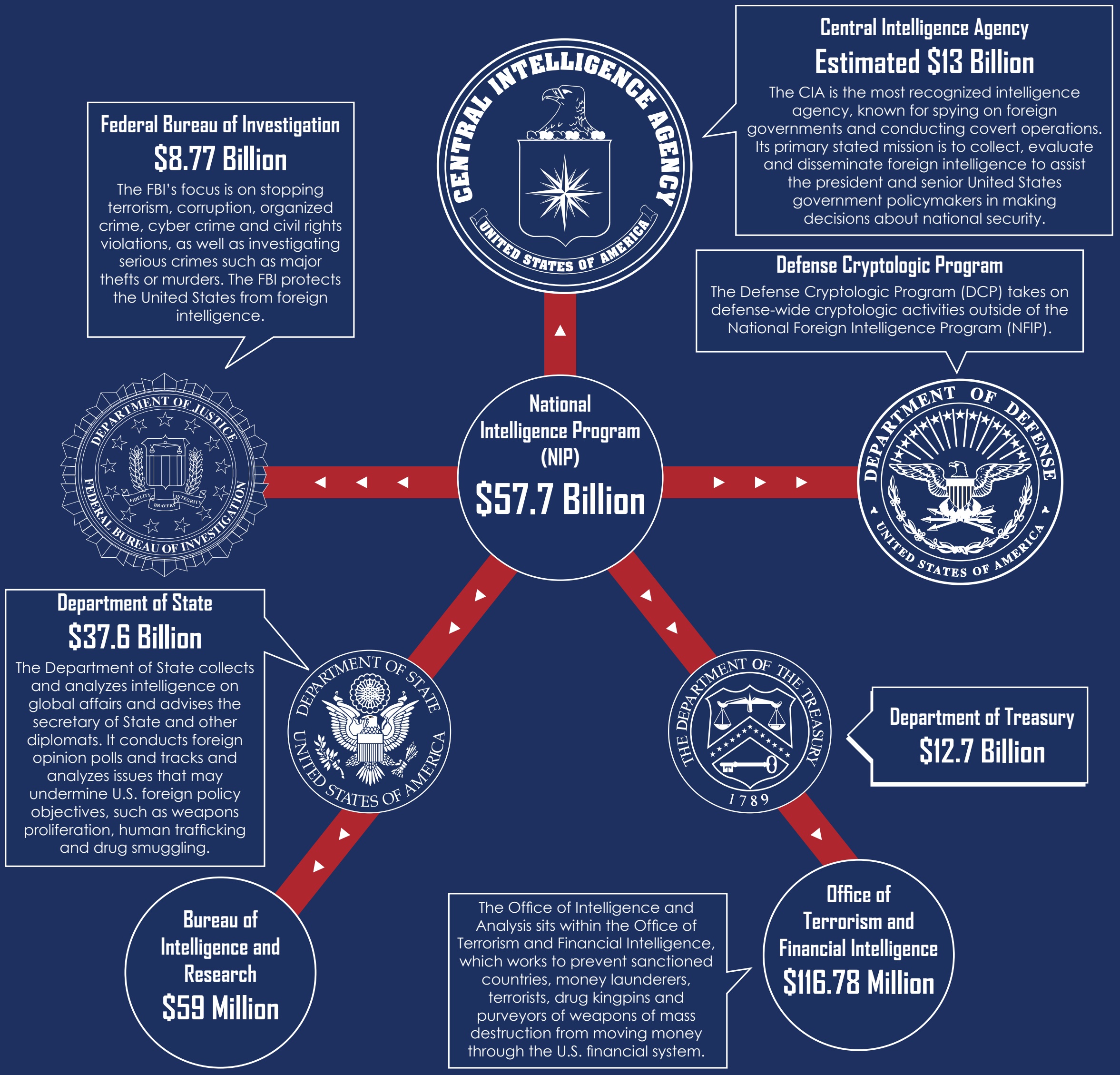
ROBOTICS

INTELLIGENCE ANALYTICS



Everything You Need to Know About the $5 Billion Increase in the U.S. Intelligence Budget for FY 2018

The United States intelligence budget comprises all the funding for the agencies of the United States Intelligence Community. This infographic details where the requested $5 billion increase in funding has been allocated. The Trump administration requested $57.7 billion for the National Intelligence Program (NIP), an increase from a requested $54.9 billion in FY 2017. The Administration additionally requested $20.7 billion for the Military Intelligence Program (MIP), up from a requested $18.5 billion in FY 2017. No other MIP budget figures or program details will be released, as they are classified for national security reasons.



National Intelligence Program (NIP)

$57.7 Billion

Central Intelligence Agency

Estimated $13 Billion

The CIA is the most recognized intelligence agency, known for spying on foreign governments and conducting covert operations. Its primary stated mission is to collect, evaluate and disseminate foreign intelligence to assist the president and senior United States government policymakers in making decisions about national security.

Federal Bureau of Investigation

$8.77 Billion

The FBI's focus is on stopping terrorism, corruption, organized crime, cyber crime and civil rights violations, as well as investigating serious crimes such as major thefts or murders. The FBI protects the United States from foreign intelligence.

Defense Cryptologic Program

The Defense Cryptologic Program (DCP) takes on defense-wide cryptologic activities outside of the National Foreign Intelligence Program (NFIP).

Department of State

$37.6 Billion

The Department of State collects and analyzes intelligence on global affairs and advises the secretary of State and other diplomats. It conducts foreign opinion polls and tracks and analyzes issues that may undermine U.S. foreign policy objectives, such as weapons proliferation, human trafficking and drug smuggling.

Department of Treasury

$12.7 Billion

Bureau of Intelligence and Research

$59 Million

Office of Terrorism and Financial Intelligence

$116.78 Million

The Office of Intelligence and Analysis sits within the Office of Terrorism and Financial Intelligence, which works to prevent sanctioned countries, money launderers, terrorists, drug kingpins and purveyors of weapons of mass destruction from moving money through the U.S. financial system.

Military Intelligence Program (MIP)

$20.7 Billion

U.S. Army Military Intelligence

The primary mission of military intelligence in the United States Army is to provide timely, relevant, accurate, and synchronized intelligence and electronic warfare support to tactical, operational and strategic-level commanders.

Airforce ISR Agency

The Air Force ISR Agency provides intelligence, surveillance and reconnaissance (ISR) products, applications, capabilities and resources, to include cyber and geospatial forces and expertise.

The Office of Naval Intelligence

The Office of Naval Intelligence mission includes real-time reporting on the developments and activities of foreign navies, protecting maritime resources and interests, monitoring and countering transnational maritime threats, and providing technical, operational, and tactical support to the U.S. Navy.

United States Special Operations Command

Its primary missions are to provide Human Intelligence (HUMINT) and Signal Intelligence (SIGINT) mainly for Delta and DEVGRU's (SEAL Team Six) operations.

Marine Corps Intelligence Activity

The Marine Corps' intelligence officers create military maps, intercept and translate radio and electronic signals, analyze images collected from sensors and carry out counterintelligence.

BOTH NIP AND MIP

National Security Agency

Estimated $10 Billion

The NSA focuses on signals intelligence, monitoring, and collecting and processing communications and electronic information. It protects U.S. information systems from outside penetration.

Defense Intelligence Agency

Estimated $4.4 Billion

The DIA is the primary entity responsible for collecting and analyzing intelligence on foreign militaries, with support from the intelligence offices of all the military branches.

National Geospatial-Intelligence Agency

Estimated $5 Billion

NGA is the provider of geospatial intelligence – analysis and information about Earth's natural and man-made features and geo-tagged activities. "GEOINT" is used for combat, humanitarian and disaster relief, border and transportation security and security planning for special events.

ARTIFICIAL INTELLIGENCE IN THE INTELLIGENCE COMMUNITY: TRENDS WITHIN ANALYTICS, THE FUTURE & MORE

INSIGHT FROM INTELLIGENCE EXPERTS

Lieutenant General (ret) Robert Otto
Former Air Force Deputy Chief of Staff for
Intelligence, Surveillance and
Reconnaissance
Chairman, Intelligence Analytics 2018

Grant Scott
Assistant Research Professor
Data Science and Analytics Masters Program
Center for Geospatial Intelligence
University of Missouri

IDGA sat down with Retired Lieutenant General Robert Otto and Assistant Research Professor Grant Scott to discuss upcoming projects, trends in artificial intelligence and machine learning, how intelligence analytics will transform in the next few years, what they are most looking forward to at the upcoming Summit and more.

Interview with Lieutenant General (ret) Robert P. "Bob" Otto

Lieutenant General (ret) Robert Otto
Former Air Force Deputy Chief of Staff for Intelligence, Surveillance and Reconnaissance
Chairman, Intelligence Analytics 2018

ABOUT

I was blessed to have a diverse Air Force career, from line F-15 pilot in my early years to leading the 27,000 men and women who make up Air Force intelligence and reconnaissance. In between those bookends I had the chance to command at the squadron, group, wing, and center level. During the dozen or so years I was a general officer, I was in the reconnaissance and intelligence business. It was exciting to train the crews and generate the sorties that gathered the SIGINT, COMINT, and GEOINT around the globe. It was especially gratifying to lead the women and men who turned that collection into intelligence. The Air Force ISR enterprise is huge, complicated, and diverse. It is also critical to the DoD and our nation, so it was an honor to play a key role.

WHERE DO YOU SEE THE FUTURE OF INTELLIGENCE ANALYTICS WITHIN THE NEXT 3 YEARS?

Analytics is rapidly transforming. Increased processing power, GPUs, availability of huge data sets, and advanced algorithms are all key reasons we are seeing an acceleration in the rate of change in analytics. The challenge for the DoD is to harness the best of what is happening in the private sector, and apply it to the defense business. It presents organizational, agility, and process challenges. Worse, there are good reasons to believe other nation states have a head start embracing new ways to looking at analytics. I think the DoD recognizes both the threat and the potential, so the next three years will be marked by experimentation, rapid development, and fielding. Training and integration will remain major challenges for all of the services and agencies.

WHAT ADVICE WOULD YOU GIVE LEADERS IN THE INTELLIGENCE SECTOR OF THE MILITARY? PRIVATE SECTOR?

Don't sit on your laurels. We clearly have many areas of excellence and world-leading capabilities. But the tectonic plates are shifting, so the landscape so familiar to the military and private sector can rapidly shift. It is more important than ever to stay abreast, and to ensure agile policies and processes to take advantage of the right opportunities.

WHAT ARE YOU MOST EXCITED ABOUT FOR THE INTELLIGENCE ANALYTICS SUMMIT?

I really look forward to the chance to learn from the varied experts that will be presenting their thoughts, ideas, best practices, and vision of the future. It is important to learn from the work of others, and understand how to apply it to similar situations. The conference will provide the chance to learn, debate, collaborate, and energize the attendees. It promises to be a meaningful three days.

Interview with Grant Scott

Grant Scott
Assistant Research Professor
Data Science and Analytics Masters Program
Center for Geospatial Intelligence
University of Missouri

ABOUT

Dr. Scott is currently a founding Director of the Data Science and Analytics Master’s Degree program at the University of Missouri (MU). He serves as the Program Manager (principal and architect) of the University of Missouri's Program of Study in Data Science training contract for the National Geospatial-Intelligence Agency and other DOD/IC customers. He currently holds a position as a Research Assistant Professor at the Center for Geospatial Intelligence and in the Department of Electrical Engineering and Computer Science at MU. He has participated in projects for NGA, DIA, Army and DARPA. He is currently mentoring or leading research projects in a number of areas including data science, computer vision, spatiotemporal analytics, high-performance computing, and Internet of Things (IoT), and crowd-sourced information mining. He also has years of industry experience in enterprise systems support and development.

ABOUT (CONTINUED)

Current research interests and areas of contribution include:

- Applying deep learning technologies to geospatial data sets for object detection;
- Data science computation engine, extensions of enterprise RDBMS with HPC co-processors;
- Real-time processing of large-scale sensor networks and Internet of Things (IoT) data;
- Crowd-source information mining and multi-modal analytics;
- High performance & scalable content-based retrieval (geospatial data, imagery, biomedical);
- Imagery and geospatial data analysis, feature extraction, object-based analysis, and exploitation.

Machine-Learning Assisted Visual Intelligence Analytics
I will recap some of the CGI past successes and our next stages of research we are pursuing.

WHAT TREND TO DO YOU SEE FOR ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING/DEEP LEARNING IN THE DEFENSE INTELLIGENCE SECTOR? WHAT ARE THE ADVANTAGES, DISADVANTAGES, OR RISKS OF USING AI WITHIN THE MILITARYAND GOVERNMENT?

I think a trend we cannot deny it that AI and Machine Learning (deep or otherwise) will continue to find their place within the defense and intelligence sectors. One of the keys to success will be constraining the goals of the algorithms to supplement and not replace the analysts and their years of tradecraft experience. One of the biggest safeguards we need to have is keeping humans in the loop, continually evaluating and quality assuring the output of advanced models and algorithms. Data and its context are continually evolving, and models must be likewise continually monitored, evaluated, and refined to stay effective.

Lieutenant General (ret)
Robert Otto

As the Chairman of Intelligence Analytics 2018, Lieutenant General (ret) Robert Otto will share his remarks throughout the entire Summit.

Grant Scott

MACHINE LEARNING AS IT ASSISTS WITH ANALYTICS

- Deep CNN processing as it relates to time, efficiency, and accuracy
- Turning AI into a force multiplier vs. a replacement

13TH
HOMELAND SECURITY WEEK

Homeland Security Week October 22-24 in Washington D.C. will bring together top homeland security leaders from government, industry and academia to dive into current challenges and future requirements necessary for numerous government agencies directly or indirectly responsible for U.S. homeland security. Through interactive keynote presentations, large scale panel discussions, project updates, case studies, and intimate roundtables, we'll facilitate a complex, joint, multilayered plan to combat the evolving challenges our country faces.

FIND OUT MORE

www.HomelandSecurityWeek.com

DIRECTED ENERGY

TRACKING THE LATEST MILITARY DEVELOPMENTS IN DIRECTED ENERGY SYSTEMS

PROGRESSING FROM RESEARCH TO IMPLEMENTATION

IDGA took a look at some of the latest developments taking place in the directed energy space. There has yet to be significant progress in directed energy weapons and although the technology for the most part is here, lasers have to get more efficient and reliable for contracts to be issued and operational implementation to begin. Congress has authorized roughly $2.4 billion on R&D work into new weapon technologies for 2018. This huge amount of funds is working to make lasers and railguns a reality. Below is a timeline of what the US Military is currently developing to maintain its status as the world's military leader.

U.S.ARMY

U.S.ARMY

2017

HIGH ENERGY MOBILE DEMONSTRATOR (HEL MD)

Back in 2014, the U.S. Army awarded Lockheed Martin a **$25 million** contract to design, construct and test a 60-kilowatt electric laser to be integrated and tested in a truck-mounted weapon system demonstrator**.** The laser weapon is designed to significantly improve the warfighters' ability to counter rockets, artillery, mortars and unmanned aerial threats. Under the contract, managed by the U.S. Army Space and Missile Defense Command's Technical Center, the laser will be integrated on the High Energy Laser Mobile Demonstrator (HEL MD). This rugged laser builds on the current Robust Electric Laser Initiative (RELI). The 60 kilowatt High Energy Laser Mobile Demonstrator (HEL MD) was delivered in 2017 for field testing.

2017

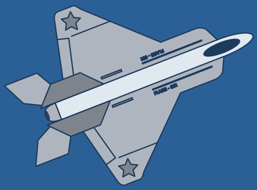
HIGH ENERGY LASER FOR U.S. ARMY APACHE AH-64

In June of 2017, Raytheon bolted a laser to a U.S. Army Apache AH-64 helicopter and zapped an unmanned target at the White Sands Missile Range in New Mexico. According to Raytheon, the weapons test marked the first time a "fully integrated laser system" had successfully located and shot a target from a rotary-wing aircraft "over a wide variety of flight regimes, altitudes and air speeds." The goal of the experiment, conducted in collaboration with U.S. Special Operations Command, was to see how well the Apache could fire the weapon given the vibration of the helicopter, the dust kicked up by the rotating blades and the vehicle's "downwash," or downward airflow.

2018

HIGH ENERGY LASER WEAPON SYSTEM ONBOARD A POLARIS MRZR

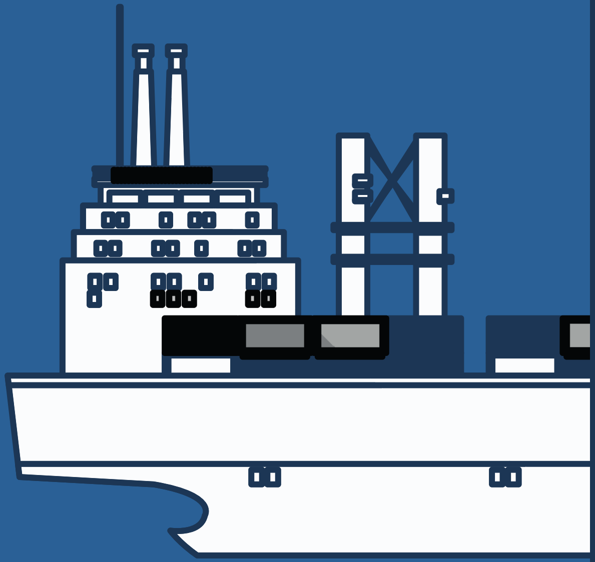
In January of 2018, Raytheon combined a high energy laser with an advanced variant of a Multi-spectral Targeting System – a sophisticated package of electro-optical and infrared sensors – and installed it on a Polaris MRZR. On a single charge from a standard 220v outlet, the HEL system onboard the Polaris MRZR delivers four hours of surveillance, intelligence, and reconnaissance capability and 20 to 30 laser shots. Raytheon began field testing the HELWS MRZR in January, and is scheduled for a demonstration at the U.S. Army's Maneuver Fires Experiment at Fort Sill, Oklahoma, in December 2018.



2021

HIGH ENERGY LASER SYSTEM FOR TACTICAL FIGHTER JETS

In 2017, the Air Force Research Lab awarded Lockheed Martin a **$26 million** contract to develop a high-energy laser system to test on a tactical fighter jet by 2021. Officials declined to specify the laser's capabilities or to identify which aircraft the service will use to test it.



2020

SURFACE NAVY LASER WEAPON SYSTEM

In January of 2018, the U.S. Navy awarded Lockheed Martin a **$150 million** contract, with options worth up to **$942.8 million**, for the development, manufacture and delivery of two high power laser weapon systems. These laser weapons will have intelligence, surveillance and reconnaissance (ISR) and counter-Unmanned Aerial System (counter-UAS) capabilities, to be complete by 2020. With the High Energy Laser and Integrated Optical-dazzler with Surveillance (HELIOS) system, the Navy take a significant step forward in its goal to field laser weapon systems aboard surface ships.

THE FUTURE OF DIRECTED ENERGY

THE IMPACT OF FY 2018 BUDGET APPROPRIATIONS, UPCOMING DEVELOPMENTS, & R&D PRIORITIES

INSIGHT FROM THE U.S. ARMY & AIR FORCE

INSIGHT INTO THE FUTURE DIRECTED ENERGY

We sat down with Colonel Richard Haggerty and Dr. Boris Zhdanov to discuss how the FY 2018 budget appropriations affected directed energy (DE) programs, where DE acquisition and force integration is heading in FY 2019, their priorities for research and development and more.

Colonel Haggerty is currently the ninth Project Manager for Instrumentation, Targets, Threat Simulators and SOF Training Systems (PM ITTS) at PEO STRI, U.S. Army. And Dr. Zhdanov currently is a Senior Scientist at the Laser and Optics Research Center (LORC) at the US Air Force Academy (USAFA).

COLONEL RICHARD HAGGERTY

Project Manager, Instrumentation, Targets, Threat Simulators, and SOF Training Systems (PM ITTS)
PEO STRI, U.S. Army

DR. BORIS ZHDANOV

Senior Scientist
US Air Force Academy

INTERVIEW WITH COLONEL RICHARD HAGGERTY

Colonel Richard Haggerty is currently the ninth Project Manager for Instrumentation, Targets, Threat Simulators and SOF Training Systems (PM ITTS) at PEO STRI, Orlando, Florida. In support of its dynamic mission, PM ITTS manages five activities: the Instrumentation Management Office (IMO), the Product Manager for Special Operations Forces Training Systems (PM STS), and the product Lead for Cyber Resiliency and Training (PL CRT) located in Orlando, Florida; and the Targets Management Office (TMO) and the Threat Systems Management Office (TSMO) located in Redstone Arsenal, Alabama.

Can you tell me a little about your role at PEO STRI?
I'm the acquisition Project Manager of a joint portfolio supporting Test, Training, Cyber and Electromagnetic Activities (CEMA), and Special Operations.

Did the FY 2018 budget appropriations affect DE programs, and what do you expect to see in the future?
Our Resource Sponsor has done what it can to support the directed energy test developments, but consistent and prolonged Continuing Resolutions and the current FY18 appropriation has impacted development and prevented the initiation of new efforts.

What direction do you see directed energy development, acquisition and force integration heading in FY 2019?
The directed energy community is leveraging mature technologies for rapid prototyping and experimentation that will expedite the fielding of directed energy capabilities into the hands of the Warfighter. Rapid prototyping also supports military utilization assessments and tactics, techniques and procedures (TTPs) development.

In your role, what are the priorities for DE research and development?
We leveraged directed energy Test and Evaluation/ Science and Technology technologies for our top priority - to develop instrumented and threat-representative capabilities. These enable open air testing of directed energy systems in operationally representative environments.

What are you most excited about for the Directed Energy Systems Summit?
Collaborating and finding synergies across the services to enable more efficient and focused fielding of directed energy into the hands of the Warfighter.

INTERVIEW WITH DR. BORIS ZHDANOV

Dr. Boris Zhdanov is Senior Scientist at the Laser and Optics Research Center (LORC) at the US Air Force Academy (USAFA). He has over 35 years' experience in research and development on solid-state lasers, molecular lasers, alkali lasers, nonlinear optics, laser spectroscopy, atmospheric propagation, and teaching at the university level. Dr. Zhdanov has over 200 publications and conference presentations. He previously worked at LORC USAFA on the Diode Pumped Alkali Lasers project.

Can you tell me a little about your role at the U.S. Air Force Academy?
I am a contractor with Air Force Academy working as a Senior Researcher at Laser and Optics Research Center (LORC) of the Academy. I involved in research project devoted to development of Diode Pumped Alkali Lasers (DPALs), which are the most promising laser for various Directed Energy applications.

Did the FY 2018 budget appropriations affect DE programs, and what do you expect to see in the future?
I think that DE programs must be better funded in future than in FY18, because development of tactical and strategic DE weapons is very important for national security and defense.

What direction do you see directed energy development, acquisition and force integration heading in FY 2019?
My opinion, that it is very important to start extensive research aimed to development of a high power laser source producing high quality beam from single aperture that allows to destroy targets at very long distance.

In your role, what are the priorities for DE research and development?
I would recommend to pay more attention and invest more funds to the development of high power DPALs scalable to power levels required for DE applications at long distances.

What are you most excited about for the Directed Energy Systems Summit?
The opportunity to deliver my thoughts to the people, who can make decision on the future of Directed Energy Systems development.

13TH HOMELAND SECURITY WEEK

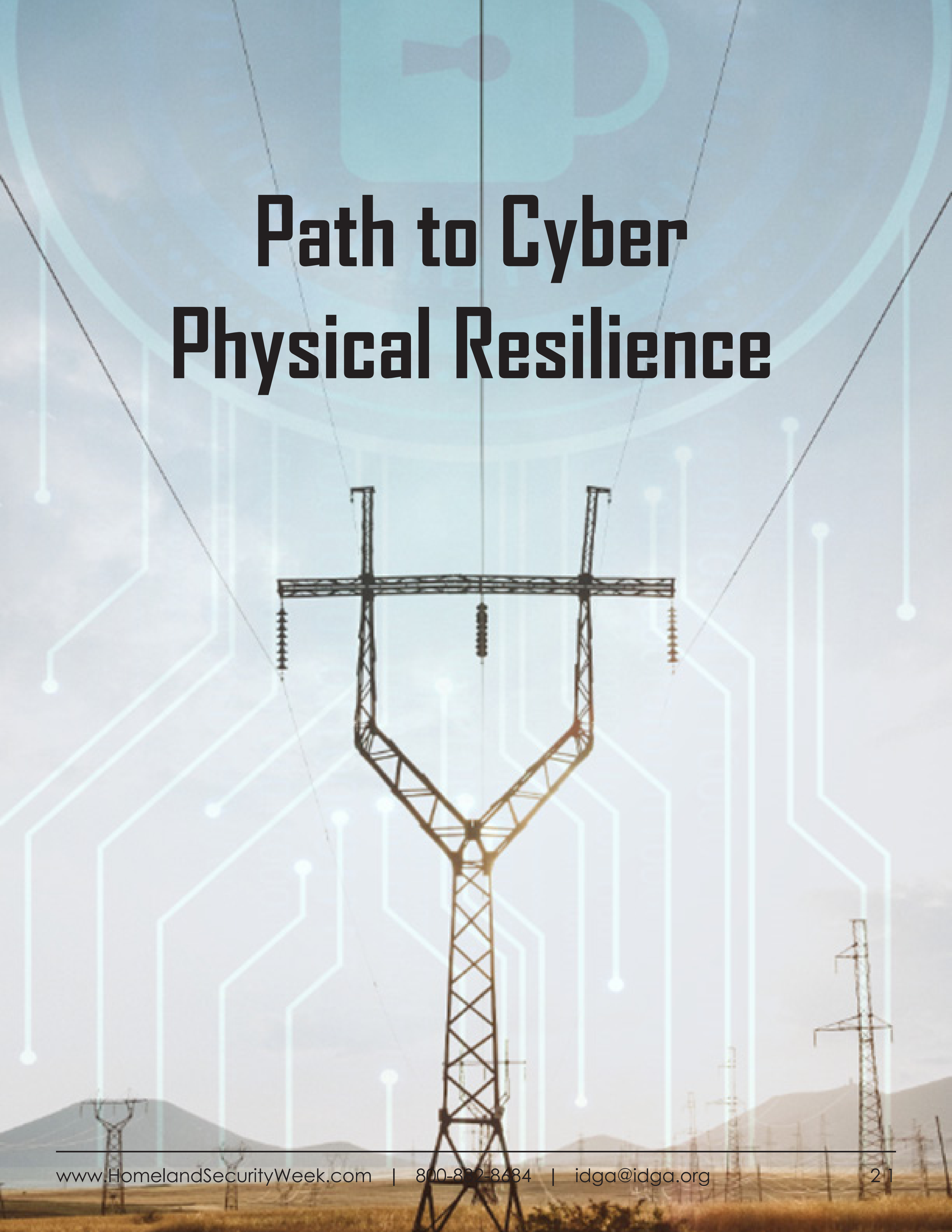
Homeland Security Week October 22-24 in Washington D.C. will bring together top homeland security leaders from government, industry and academia to dive into current challenges and future requirements necessary for numerous government agencies directly or indirectly responsible for U.S. homeland security. Through interactive keynote presentations, large scale panel discussions, project updates, case studies, and intimate roundtables, we'll facilitate a complex, joint, multilayered plan to combat the evolving challenges our country faces.

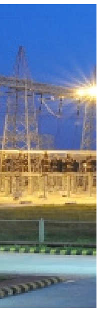
FIND OUT MORE

www.HomelandSecurityWeek.com

CRITICAL INFRASTRUCTURE

Path to Cyber Physical Resilience





Integrating Cyber & Physical Security

The convergence of physical and ICT Information and Communications Technology) systems has created a variety of new opportunities. There have been improvements in enhanced reliability and reaction time. Utilities companies are discovering that a key enabler of a flexible grid is the ability to apply information and communication technology (ICT) to electric transmission and distribution systems.

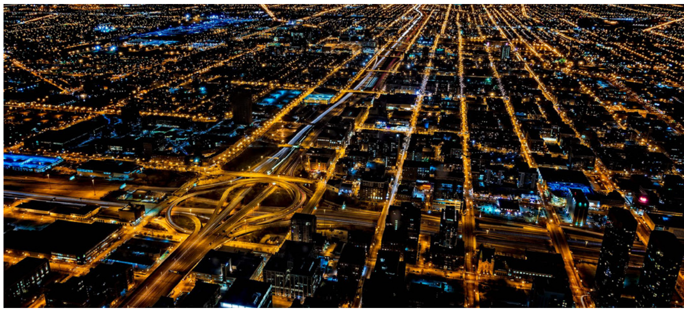
A number of ICT's enable power grid companies to achieve a greater level of flexibility, which is desired to meet the needs of today's business environment. This includes the deployment of communication technologies to field devices, evolving standards and protocols, cybersecurity measures to address the threats to an interconnected grid, data analytics, and enterprise architecture applied to electric grid physical technology. Each of these ICT areas can be applied to address industry needs, such as wide area situational awareness, operations and planning and mobility to accommodate increased numbers of distributed energy resources on the distribution system, as well as to advance operations and decrease system restoration times during major physical and cyber events.

The integration of cyber and physical systems is making major improvements in the capability to monitor and operate the grid, as well as offering improved protection. But at the same time, it is also introducing new weaknesses. To reduce existing vulnerabilities and minimize the introduction of new ones, cyber and physical expertise must be integrated into all stages of the research develop-build-operate continuum. Additional integration is needed when existing systems are upgraded or repaired, not just when new technology is introduced.

The integration of cyber and physical systems is making major improvements in the capability to monitor and operate the grid, as well as offering improved protection.

This is because such changes can introduce unrecognized vulnerabilities if both overall systems and components are not evaluated before changes are made. Increased communications between technology developers, suppliers, integrators, and buyers on how the systems will be used, could help improve their understanding of security implications and, therefore, result in better solutions to prevent interruptions to an interconnected grid.

Business Drivers for Convergence



While convergence does present some new vulnerabilities, specifically cyber related threats, it provides new opportunities for grid-associated value streams, enhanced system performance, and additional options for consumer interaction with utilities systems.

Specifically, there are five main business drivers for grid convergence:

1 The growth of the digital grids are resulting in the deployment of millions of new intelligent grid devices into a distribution network— including smart meters, line sensors and on-load tap changers—all generating important information across all parts of the business.

2 The growing complexity of handling distribution networks is motivating utilities to look for improved approaches to optimize their systems, such as integrating real-time weather information into distributed generation management and automated rule-based control of assets.

3 Innovative business models are producing services that can only be delivered when business data and operational decisions are brought together, such as the purchase of network services from third-party storage operators.

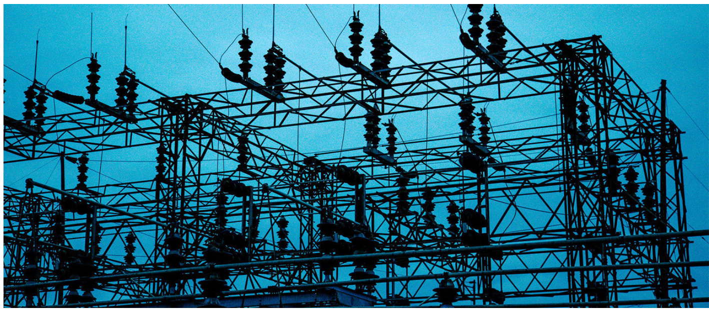
4 Regulators are pushing utilities to do more with less. At the same time, in many mature countries, overall energy consumption is flat or declining while peak demand remains constant or is increasing—thereby additionally straining distribution assets while weakening traditional energy consumption-based cost recovery models.

5 New distribution assets delivered with noteworthy embedded sensor technologies, combined with communications and analytic technologies, can yield faster, more accurate insights that optimize and extend asset life.

Three out of four executives shared that the area with the greatest potential for benefits was enhanced decision making results from the analysis of operational data. Capabilities such as enterprise asset management, network planning and workforce management would clearly benefit from more granular, timely data from the operational systems. It is clear that executives expect convergence to support the core business capabilities, making better use of internal and external data sources to improve decision making and provide better service levels.

Convergence is also expected to provide some back-office benefits as well, such as reducing manual hand-offs that can be time-consuming and error-prone.

Priorities Within Convergence



There are three areas that have been rated as the highest priorities:

Unplanned Outage Management

For most utilities, the current process to respond to an outage and restore power is a significant driver of cost. It requires a number of processes, each of which must follow in order, with relevant information managed through a series of "handshakes" and "hand-offs" between control rooms, dispatchers and maintenance crews. Being able to enrich situational awareness across that sequence with data that addresses fault identification, location and fault data from various sources as well as information about crew availability and proximity to an event can help utilities achieve significant savings. More sophisticated data can even identify and analyze the optimal deployment of crews to avoid excessive overtime payments. Management of unplanned outages can also be significantly improved by more effective automation and planning that is made possible by integrating data from multiple sources.

Asset Management

Monitoring asset health and performance in real-time could enable utilities to make more effective engineering decisions, as well as plan and allocate capital expenditure more accurately and effectively. That ability will become increasingly important as regulatory funding becomes more incentive and performance-based. The ability to successfully harness data within asset management planning will require analytic tools and skills that most utilities currently lack. But these tools and skills will be essential for distribution companies to move successfully from planning policies based on largely historic statistical models to nearer realtime data that can support more granular, asset- and circuit-specific actions and interventions.

Integrating Distributed Generation Through Monitoring & Control

The integration of cyber and physical data will be essential for distribution companies to achieve more efficient integration of distributed generation (DG), limiting the requirements for large capital reinforcement spend or any adverse impacts to the network reliability. These smart approaches to DG integration require the availability and analysis of considerable flows of data. Currently, that data is not often readily available, particularly for small-scale DG. Many distribution companies, for example, have little if any visibility into prosumer systems across the grid and have to estimate the size and timing of DG exports to the grid. Yet, utilities expect to see grid faults increase substantially by 2020 as a result of the expansion in DG technologies.

Design & Development

Significant research is underway on the design and development o f new and improved grid technologies. A majority of the research is being driven by investments to increase reliability, improve operational efficiency, and accommodate changing generation sources.

Two areas deserve supplementary attention, both of which were noted in the Energy Sector-Specific Plan. A comprehensive framework for interdependency modeling and simulation to help (1) integrate the multiple and disparate models, tools, and simulations that already exist for different infrastructure; and (2) facilitate cross-sector analysis to address the threat assessment, protection, mitigation, response, and recovery issues associated with interdependencies.

Long-term research and development is required to make power grid technologies more resilient through more integrated designs that support quick(er) replacement, more flexible and adaptable designs that speed recovery, self-healing systems to minimize outages and damage, and so on. There is also a necessity for research and development to improve response to, and recovery from, adversarial incidents (as well as other types of incidents).

Noteworthy cybersecurity work is also ongoing through DOE's Cybersecurity for Energy Delivery Systems (CEDS) program intended to assist the energy sector asset owners (electric, oil, and gas) by developing cybersecurity solutions for energy delivery systems through integrated planning and a concentrated research and development effort. CEDS co-funds projects with industry partners to make improvements in cybersecurity competencies for energy delivery systems. Overall, it will take significant additional investment to outpace threats; this cannot be done by government alone, so the government should consider policies to reduce barriers to industry investment in grid security.

Cybersecurity Threats

In this past presentation, Mark Weatherford, the Chief Cybersec urity Strategist at vArmour, discusses the current threats to cyber-security, including foreign countries, espionage and hacktivist actors, and inside threats, as well as different ways to stop them.

The bad news . . .

Most companies are out-matched in their ability to combat cyber-attacks from nation states, global criminals and malicious insiders.

In no other arena are private sector organizations expected to do battle with the likes of:

- Izz ad-Din al-Qassam Cyber Fighters
- The Syrian Electronic Army
- North Korea's Bureau 121
- Russia's Sandstorm Crew
- China's 13638 group
- Anonymous
- Sandworm Team
- Lizard Squad
- Comment Crew
- AnonGhost

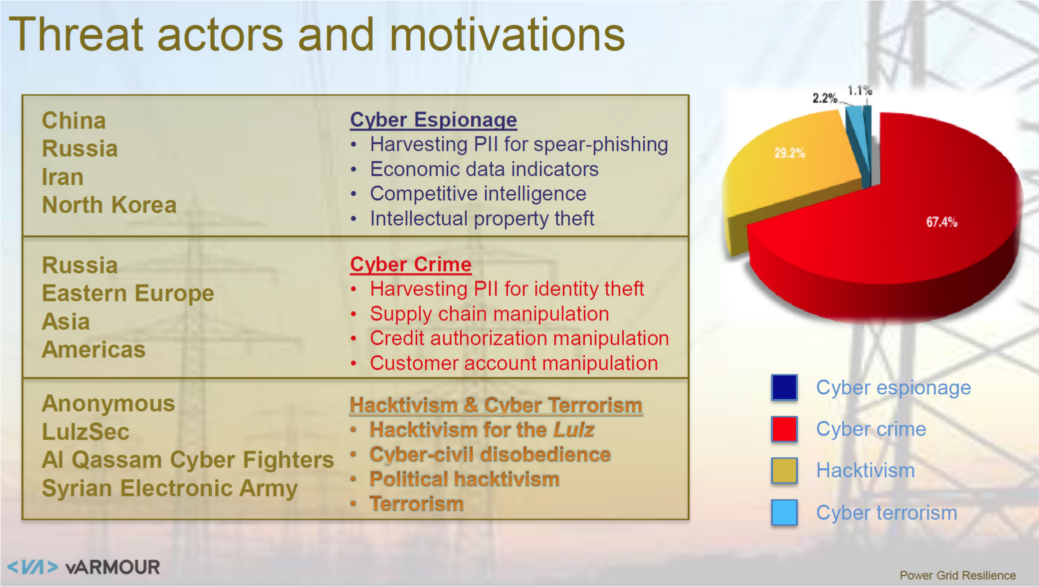
They don't understand…

"The power grid is designed to be vulnerable to "cascading failures." This is how it maintains continuous service in the face of inevitable component failures.

While the resilience of the system is continually improving, there will always be an upper bound to the number of simultaneous component failures that the system can tolerate. When that threshold is crossed, apparently about once a generation, the system is designed to shut down in an orderly and non-destructive manner.

These successful shutdowns enable the system to resume normal service in hours to tens of hours. Such successful shutdowns will continue to be described by politicians and the media as "failures." The designers and operators of the network will continue to think of them as "power grid security."

- Dr. William Murray



Threat actors and motivations

China Russia Iran North Korea	**Cyber Espionage** • Harvesting PII for spear-phishing • Economic data indicators • Competitive intelligence • Intellectual property theft
Russia Eastern Europe Asia Americas	**Cyber Crime** • Harvesting PII for identity theft • Supply chain manipulation • Credit authorization manipulation • Customer account manipulation
Anonymous LulzSec Al Qassam Cyber Fighters Syrian Electronic Army	**Hacktivism & Cyber Terrorism** • Hacktivism for the *Lulz* • Cyber-civil disobedience • Political hacktivism • Terrorism

🟦 Cyber espionage
🟥 Cyber crime
🟨 Hacktivism
🟦 Cyber terrorism

Cyber approach to risk management

Strategy: Managing Risk for Present & Future

- We face an adaptive threat in a changing regulatory environment – frame risk accordingly
- Not everything requires the same level of security
- Make security a business enabler

Governance: Inspect, Don't Just Expect

- Help Executive Leadership understand cyber risks and define their role in managing those risks
- Build a centralized planning process – drive security into the technology lifecycle
- Ensure planning addresses risk aggregation (e.g., outsourced IT, partners, etc.)
- Use audits and metrics to monitor implementation, effectiveness and impact
- Invest in incident preparedness and incident response

Architecture and Operations: If You Can't See It, You Can't Protect It

- Build intuitive approach to controls; implement in phases
- Ensure qualified personnel are available to implement and manage the controls
- Institute continuous cycle of training and exercises

Cyber-threat intelligence risk

Organizations face three primary challenges in their intelligence-driven risk management activities

1 Information Overwhelm Information can rapidly accumulate in a way that overwhelms an organization's ability to act on it. The 3 V's problem – Volume, Velocity, and Variety of data.

2 Lack of Context Information sources from numerous point solutions (e.g., antivirus, firewalls, intrusion detection and prevention systems) are often narrowly focused and are not reported in the context of the broader operating environment

3 Lack of Correlation Information sources manifest in many different formats at network-speeds, making it difficult to correlate and extract timely, operationally relevant intelligence

Convergence

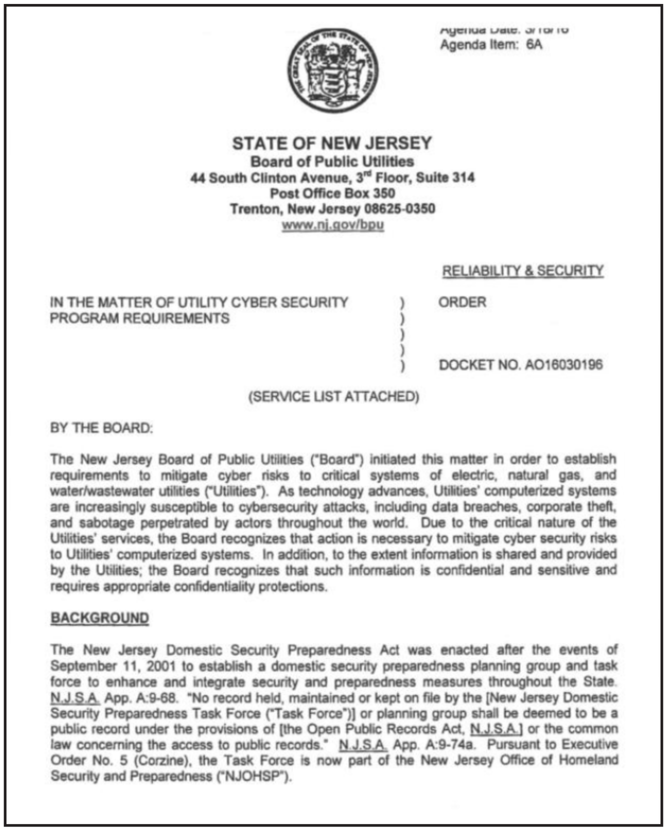
Cybersecurity convergence refers to the concept of bringing three disciplines together to manage the threats facing the electric utility industry.

- Physical security
- Cybersecurity (IT Security)
- Operational technology security (Industrial Control System and SCADA security)

Public Utility Cyber Security Program Requirements

Cybersecurity Requirements: Utilities must have a Cyber Security Program that defines and implements organizational oversight, accountabilities, and responsibilities for cyber risk management activities, and that establishes policies, plans, processes, and procedures for identifying and mitigating risk to critical systems to acceptable levels. Additionally, the Cyber Security Program must meet the following minimum requirements:

1. Cyber Risk Management
2. Situational Awareness
3. Incident Reporting
4. Response and Recovery
5. Security Awareness and Training



Agenda Date: 3/18/16
Agenda Item: 6A

STATE OF NEW JERSEY
Board of Public Utilities
44 South Clinton Avenue, 3rd Floor, Suite 314
Post Office Box 350
Trenton, New Jersey 08625-0350
www.nj.gov/bpu

RELIABILITY & SECURITY

IN THE MATTER OF UTILITY CYBER SECURITY PROGRAM REQUIREMENTS) ORDER
)
)
)
) DOCKET NO. AO16030196

(SERVICE LIST ATTACHED)

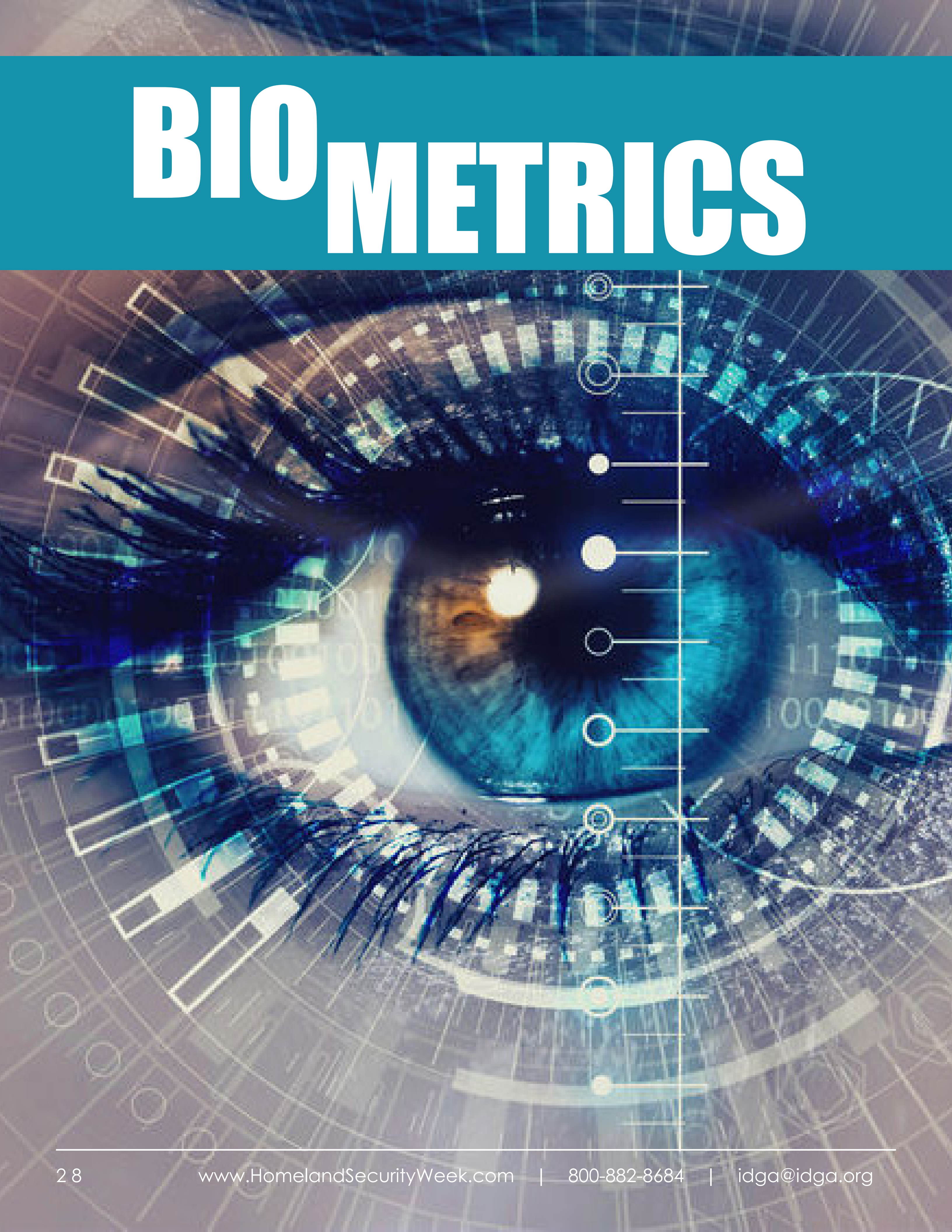
BY THE BOARD:

The New Jersey Board of Public Utilities ("Board") initiated this matter in order to establish requirements to mitigate cyber risks to critical systems of electric, natural gas, and water/wastewater utilities ("Utilities"). As technology advances, Utilities' computerized systems are increasingly susceptible to cybersecurity attacks, including data breaches, corporate theft, and sabotage perpetrated by actors throughout the world. Due to the critical nature of the Utilities' services, the Board recognizes that action is necessary to mitigate cyber security risks to Utilities' computerized systems. In addition, to the extent information is shared and provided by the Utilities; the Board recognizes that such information is confidential and sensitive and requires appropriate confidentiality protections.

BACKGROUND

The New Jersey Domestic Security Preparedness Act was enacted after the events of September 11, 2001 to establish a domestic security preparedness planning group and task force to enhance and integrate security and preparedness measures throughout the State. N.J.S.A. App. A:9-68. "No record held, maintained or kept on file by the [New Jersey Domestic Security Preparedness Task Force ("Task Force")] or planning group shall be deemed to be a public record under the provisions of [the Open Public Records Act, N.J.S.A.] or the common law concerning the access to public records." N.J.S.A. App. A:9-74a. Pursuant to Executive Order No. 5 (Corzine), the Task Force is now part of the New Jersey Office of Homeland Security and Preparedness ("NJOHSP").

BIOMETRICS



Defining Person Centric Identity Management Systems and What You Need to Know

Identity has become a core vehicle that enables governments, commercial enterprises and individuals to conduct a diversity of business functions such as financial transactions, transit across national borders, enforce laws, transfer monies, secure infrastructure, and access personal and government devices. Pillars of success require that identity be both private and secure.

National and business identity management in the past involved credentials and biographic identifiers such as name, address, date and place of birth. Today's increasingly globalized and digital world is demanding that biometrics, coupled with biographics, become the identity management standard. As a practical matter, reducing all the possible ways an individual can be identified to a simple set of attributes that, as unequivocally as possible, identify an individual as unique, checks the boxes for both government security and personal privacy.

How to do that is the question.

Unique Identity is a concept that ensures that one person has one identity in a given population, and that the one identity corresponds to one and only one person. We call systems based on Unique Identity "Person Centric biometric identity management systems (PCBIMS)." PCBIMS are emerging answer for varieties of transactions by a variety of entities requiring identity verification to be harmonized successfully, and that is the focus here.

Identity systems with policies and technologies based on Unique Identity are evolving into viable core capabilities across the world. PCBIMS success stories include India, Pakistan, and Indonesia. The most renowned Person Centric identity management system (PCBIMS) is India's Aadhaar system, where 99 percent of adult Indians hold an Aadhaar ID that links to some 84 government services, which will soon include the world's largest welfare program. The Aadhaar PCBIMS is saving the Indian government about $2 billion a year. Europe, Japan, Australia, Singapore, and many more countries, have implemented some form of Unique Identity for border management, and over 40 nations today have biometric border programs, many of which are entry/exit programs that include Unique Identity. One system alone has 210 million enrolled identities.

The Schengen EU-VIS system processes fingerprint-based visas for the 28 member countries of the European Union based on the Unique Identity concept. Asian banks have begun to use Unique Identity to reduce fraud and improve customer service. Biometric banking platforms in the Middle East support anti-corruption efforts while enabling financial inclusion in third world countries at an unprecedented level using PCBIMS.

The United States Department of Homeland Security will be modernizing its biometric identity management system that supports border and law enforcement functions to a person centric model beginning in 2018.

Where a business or national security situation requires one person to have one identity within a given population and function, PCBIMS is an opportune choice worthy of consideration.

Person Centric System Attributes

Systems that support Unique Identity have the following characteristics:

1. Unique Identity systems, by definition, do not require any specific identity credentials, but rather, can adapt to whatever credentials are provided by the enrollees. The key capability is to de-duplicate new enrollments versus existing enrollment based on biometrics, not requiring the use of a credential to validate the actual identity. Credentials may be used in concert with the biometric to link to an identity file, but are not required to verify the identity itself.

2. Scalable, accurate biometrics must be used in the system. At present, fingerprint, face, and iris are the most widely used Unique Identity system biometrics, with face still at the risk for false matching.

3. Multiple modalities of biometrics greatly improve accuracy and can increase performance for identification and deduplication. Only one modality may be required for verification, but having multiple modalities allows for flexibility upon verification.

4. Capture of biometrics and related identity credentials must be done at trusted encounters with oversight of officers at borders, banks, or airports to deter spoofing and help correct ` mismatch adjudications.

5. Each transaction should typically three services: document check, identify, and verify. The backend IDMS must be highly available, scalable, responsive, and accurate, conforming to relevant biometric and identity management standards.

6. Underlying data stores for these systems must not only be encrypted and stored under secure conditions, but (1) the biometrics, (2) the core identifying attributes, and (3) the functional identities created as a result of unique identity (e.g. a case file for an air traveler account in India), must be stored in separate data stores to preserve the privacy of each individual's data by preventing unauthorized mining of information.

PCBIMS are perceptibly changing the way people interact with their governments, businesses, and each other. Yet with such rapid growth, concrete guidance as to how to architect a BIMS for success lacks understanding.

Critical "must-haves" of any PCBIMS architecture, and the policies to enable all stakeholders to support its development, must be embraced at inception, no matter its purpose, in order to achieve success and avoid failure.

2018: Three Predictions for Biometrics in Law Enforcement

Where is advancement coming from for biometrics in law-enforcement?

Even some of the brightest biometrics minds out there have perhaps not realized that biometrics as a science has existed for hundreds of years! One school of thought dates it's origins back 700 years to China; and another attributes it to the Persians a couple of hundred years ago. Regardless of where our loyalties lie about its considerably established origins, we all perhaps agree that the earliest forms of biometrics that existed in a framework that we still know today, is fingerprinting.

While the official use of biometrics probably preceded fingerprints, the need for them, was, in our opinion, the first push for a solid and dependable set of characteristics that help in the most common use of biometrics – identification.

Fingerprinting was the birth of modern biometrics.

Before that, biometrics did exist. Perhaps not as reliably, however.

Think back to how people were sorted in various instances by their visibly distinguishing physical characteristics. One example would be when the early immigrants first came to America. They were sorted by factors like gender, height, weight, and age, as well as more distinguishing and unique features like the colour of their eyes and hair.

Not all those factors are created equal, we realized as a discipline! Some of them are features that change over time and lend themselves to disguising. Some others are constant, and much more desirable as a dependable biometric.

That was why the fingerprint became the definitive method of identification for a very long time.

Evolution has come quickly to the field of biometrics and nowhere is it seen more than in law enforcement.

So we moved, over the years, from how someone's eyes looked to the distance between their pupils as a much more reliable way of finding them.

The growth in the field, despite its adoption being far from mainstream, has been rapid. Currently, growth is being forecast to come from corporate applications. Corporate security, with the exception of facilities like airports have been slower in their adoption of biometrics.

That is about to change; a phenomenon that's set to drive a doubling in size of the biometrics market.

So where are the advances coming from?

We think the next wave of advancement for biometrics will come from a social context.

How?

1 – Easier access and user-generated data will make facial recognition more effective than ever before. Law enforcement authorities now have access to the FBI's growing facial recognition database which they are able to use for several purposes, including comparing the faces of suspected criminals to their driver's license and ID photos. Facial recognition systems today are becoming much more sophisticated. Mobile biometrics makes it much easier for agents to have access in the field to the tools they need to speed up processing of human identification (via smartphones and other mobile devices). Biometric functionality is achieved on a mobile device either through its built in biometric sensors or by attaching portable biometric hardware to it via a USB cable or Wi-Fi.

When you combine access with user-generated data, the efficiency takes a whole new turn. Criminal ID solutions are crime analysis tools that form an all-encompassing ecosystem of tools that can be utilized for crime resolution. These are called 'integrated systems' and can unify centralized crime data databases with data mining algorithms to help with analysis of crime pattern detection.

'Facebook and Google already have collected enough data and perfected algorithms to distribute information that can fill in missing faces in the FBI and local department facial recognition library; however, privacy concerns have limited the collection of information to date. As improved facial recognition for law enforcement moves full speed ahead, the next 5 to 10 years will bring near-perfect and robust facial recognition abilities, along with laws that accommodate the use of data for law enforcement purposes.'

2 – Collaborative and predictive analytics will be employed for prevention and punishment. Ethical grey area notwithstanding, 'DNA shaming', or using someone's DNA to link them to a crime and bringing them justice could soon be in effect. One example was 'the 'Face of Litter' ad campaign that went viral a couple of years back. As a way to crack down on litter, Hong Kong partnered with Ogilvy advertising and Parabon Nanolabs (using technology developed in partnership with the Department of Defense) to deploy technology that identified physical characteristics of a litterbug.

The technology took a two-dimensional look at DNA, and without identifying a person specifically, extrapolated portraits sing DNA found on pieces of litter and posted the images in public places to shame the litterbugs. This technology was crude in 2015 and purposely limited, but it is just the beginning of what DNA shaming can lead to.' New biometric identifiers in the FBI's 'Next Generation Identification' program are intended to advance the bureau's biometric identification services beyond fingerprints alone into a multimodal biometric database. Other modes include voice, iris and facial recognition. Once fully deployed, the new initiatives will promote a high level of information sharing, support interoperability, and provide a foundation for using multiple biometrics for positive identification. The existing database currently holds iris scans and DNA samples, but the newly updated database will also contain tattoos.

Another proposed element of an updated database includes an image matching service. Images of a person of interest from security cameras or photos accessed from sources such as the Internet could be compared against a national repository of images held by the FBI.

3 – These will be supported by an advancement in Behavioral Biometrics or the measure of uniquely identifying and measurable patterns in human activities.

Today's behavioral biometrics go way beyond signature, voice, and speech, into analyzing multiple data and endpoint interactions like hand-eye coordination, pressure, hand tremors, navigation and other finger movements. With these, you can tell how well people know the information they are entering and how familiar they are with the application they are using by how they engage with it.

CYBER SECURITY

EVERYTHING YOU NEED TO KNOW ABOUT THE $583 MILLION INCREASE IN CYBERSECURITY FUNDING FOR 2019

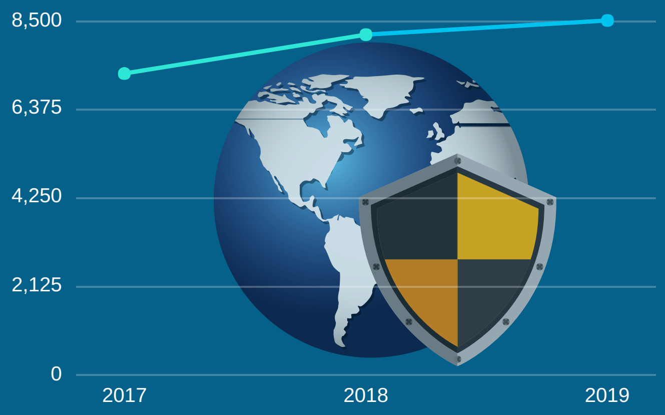
Prior to the upcoming **Cyber Security for Defense Summit** this June 25th – 27th in Washington DC, we took a look at the top ten departments scheduled to receive the most additional funding for cybersecurity in 2019. This infographic shares where these departments are looking to spend in 2019, as well as how much their cybersecurity budgets have increased over the last few years. The FY 2019 President's Budget includes $15 billion of budget authority for cybersecurity-related activities, which is a $583.4 million (4.1 percent) increase above the FY 2018 Estimate. This amount does not represent the entire U.S. cybersecurity budget, as some funding is classified.

DEPARTMENT OF DEFENSE

- The Department of Defense accounts for the largest share of the total U.S. cybersecurity budget, with a reported $8.5 billion in cyber funding in FY 2019, which is a $340 million (**4.2 percent**) increase from 2018.
- This funding will go towards activities such as the Pentagon's efforts to defeat enemy cyber attacks against U.S. forces and the military's abilities to conduct cyber warfare against existing and potential adversaries.

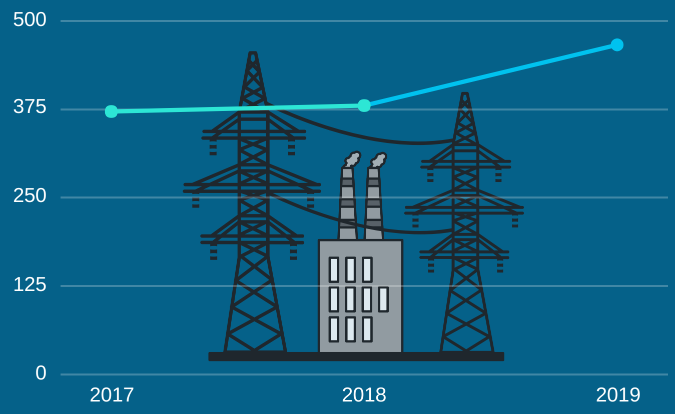
↑ **$340 Million**

2018 Estimate: $8.157 Billion
2019 Request: $8.497 Billion



⬆ $85.9 Million

2018 Estimate: $ 379.00 Million
2019 Request: $ 464.90 Million



DEPARTMENT OF ENERGY

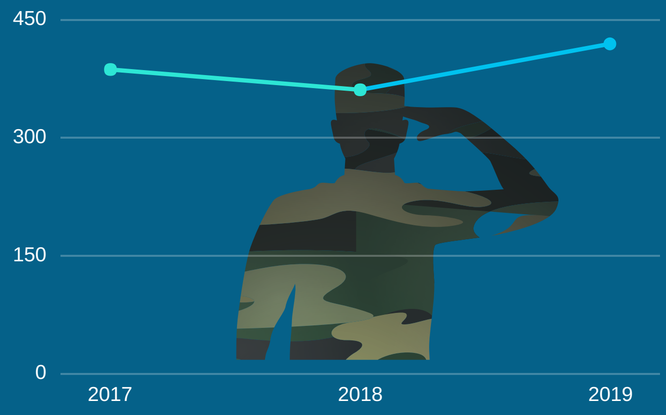
- The budget for FY 2019 requests $464.9 million in cyber security funding, which is a $85.9 million (**22.6 percent**) increase from 2018.
- A part of this increased funding will go towards creating a new office to monitor and improve the energy sector's cybersecurity- the Office of Cybersecurity, Energy Security, and Emergency Response (CESER). CESER will focus on energy infrastructure security and will support the expanded national security responsibilities assigned to the DoE.

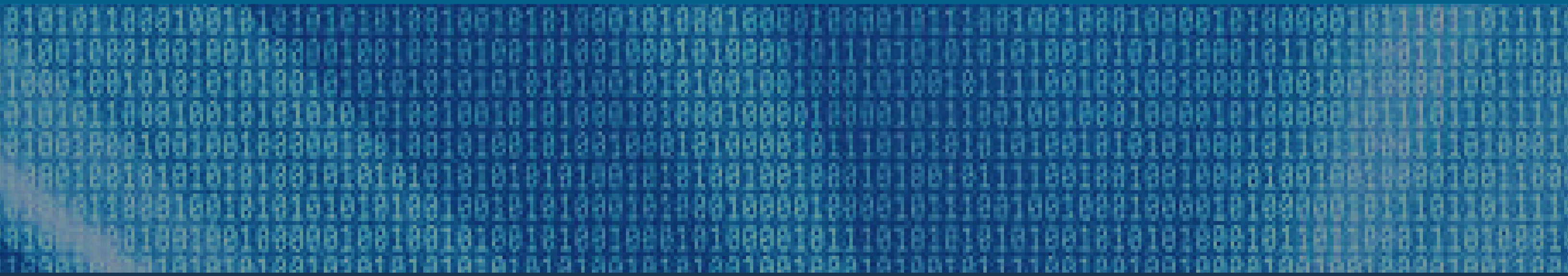
DEPARTMENT OF VETERAN AFFAIRS

- The Department of Veterans Affairs (VA) receives an increase of $58.4 million (16**.22 percent**) for FY 2019.
- This funding will go towards supporting, maintaining, and implementing cyber security requirements as they evolve. As well as improving service delivery and improving the overall security and resiliency of the underlying VA infrastructure.

⬆ $58.4 Million

2018 Estimate: $ 360.00 Million
2019 Request: $ 418.40 Million

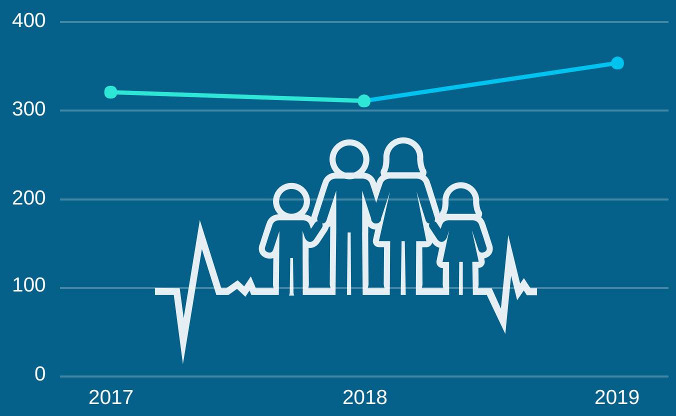




DEPARTMENT OF HEALTH AND HUMAN SERVICES

↑ $42.7 Million

2018 Estimate: $ 309.90 Million
2019 Request: $ 352.60 Million



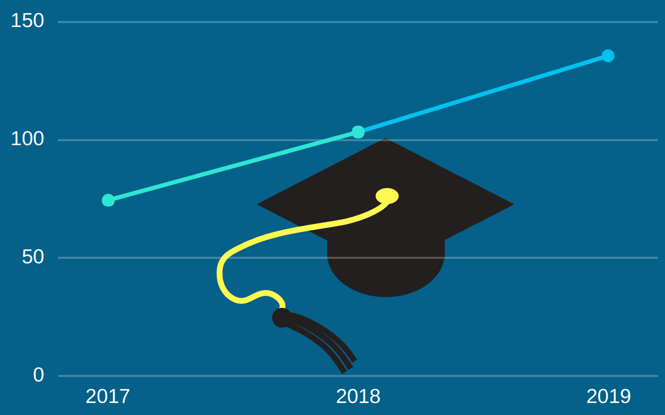
- The budget for FY 2019 requests $352.60 million, an increase of $42.7 million (**13.78 percent**) from 2018.
- This funding will go towards continuing robust operations to meet today's cybersecurity needs and ensuring the department is able to protect sensitive and critical information. This investment will help to continue operations for detecting, managing, and remediating cybersecurity risks.

DEPARTMENT OF EDUCATION

↑ $32.3 Million

2018 Estimate: $ 103.00 Million
2019 Request: $ 135.30 Million

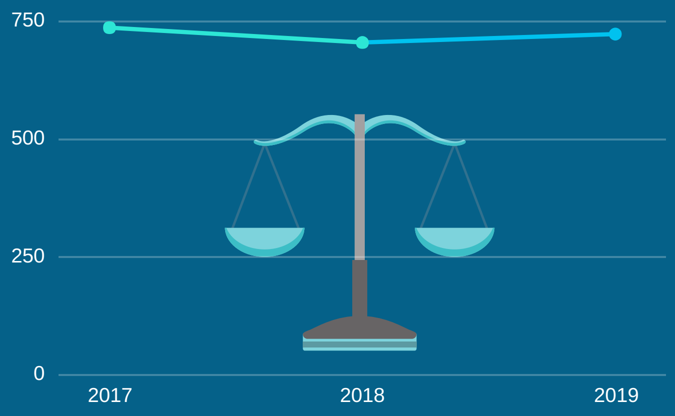
- The budget for FY 2019 requests $135.30 million, an increase of $32.3 million (**31.36 percent**) from 2018.
- The increase in funding will place focus on key departmental policies and management priorities, such as continuing improvements to the department's IT security to ensure the integrity of DoE data and to prevent potential IT security breaches.



↑ $17.8 Million

2018 Estimate: $ 703.60 Million
2019 Request: $ 721.40 Million

DEPARTMENT OF JUSTICE



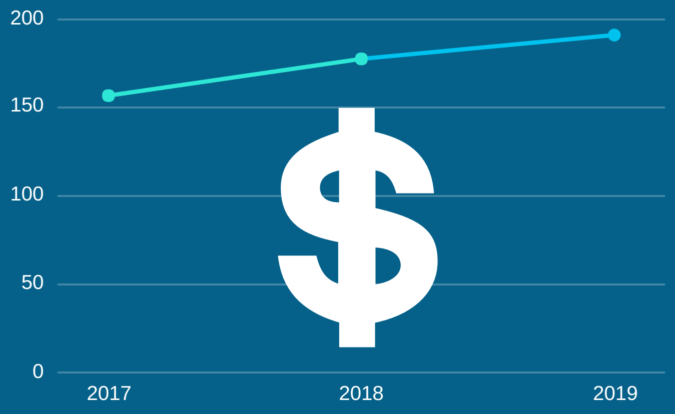
- The budget for FY 2019 requests $721.40 million, an increase of $17.8 million (**2.53 percent**) from 2018.
- The enhanced budget will go towards supporting a wide range of missions that include national security, law enforcement investigations, prosecution and incarceration. For each of these critical missions, the systems that support them must be secured to protect the sensitive information, the availability of data and workflows crucial to mission execution, and the integrity of data guiding critical decision-making.

SOCIAL SECURITY ADMINISTRATION

↑ $13.5 Million

2018 Estimate: $ 177.10 Million
2019 Request: $ 190.60 Million

- The budget for FY 2019 requests $190.60 million, an increase of $13.5 million (**7.62 percent**) from 2018.
- The increased budget will help the department's cybersecurity program in continuing to improve the agency’s detection, protection, and intelligence capabilities against evolving threats and cyber-attacks. This program incorporates security capabilities into a comprehensive, multi-layered defensive approach, ensuring the privacy of the public and proper issuance of nearly a trillion dollars in benefits.

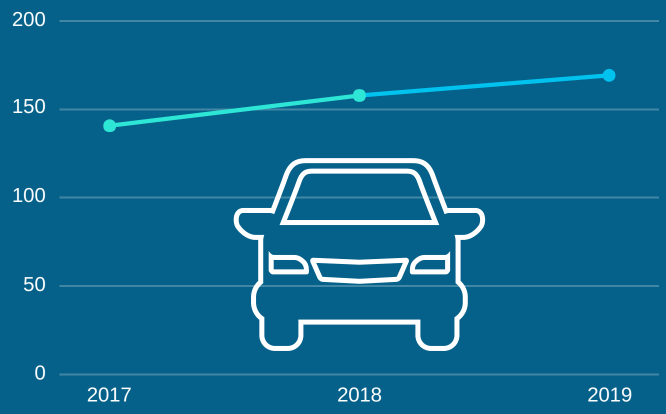


DEPARTMENT OF TRANSPORTATION

↑ $11.4 Million

2018 Estimate: $ 157.30 Million
2019 Request: $ 168.70 Million

- The budget for FY 2019 requests $168.70 million, an increase of $11.4 million (**7.25 percent**) from 2018.
- The increased budget will help to strengthen the department's ability to identify and remediate cybersecurity risks through advanced data collection, integration and reporting, and continuous monitoring.

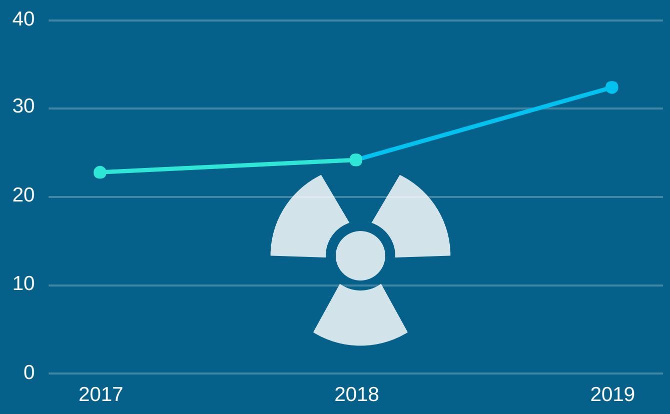


NUCLEAR REGULATORY COMMISSION

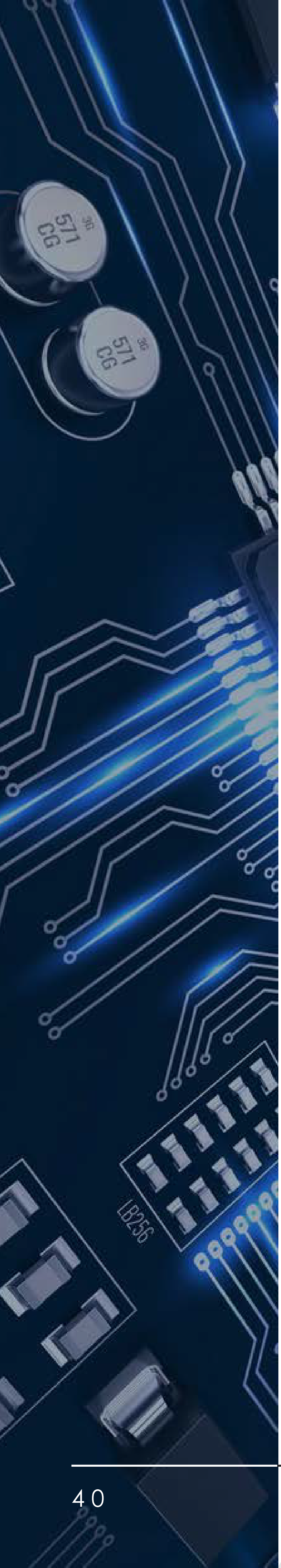
↑ $8.2 Million

2018 Estimate: $ 24.10 Million
2019 Request: $ 32.30 Million

- The budget for FY 2019 requests $32.30 million, an increase of $8.2 million (**34.02 percent**) from 2018.
- The increased budget will help to address network vulnerabilities and updates to the commission's cybersecurity policies and procedures. The 34 percent hike in funding is tied to recent events that have highlighted the growing cyber threat against nuclear plants.



ROBOTICS



The Army's Priorities for Robotic and Autonomous Systems (RAS)

Near-Term, Mid-Term, Far-Term

NEAR-TERM (2017-2020)

The Army's primary near-term investments are in pursuit of autonomous technology development.

Near-Term Priorities

The Army matures concepts and initiates or continues programs.

Strategies

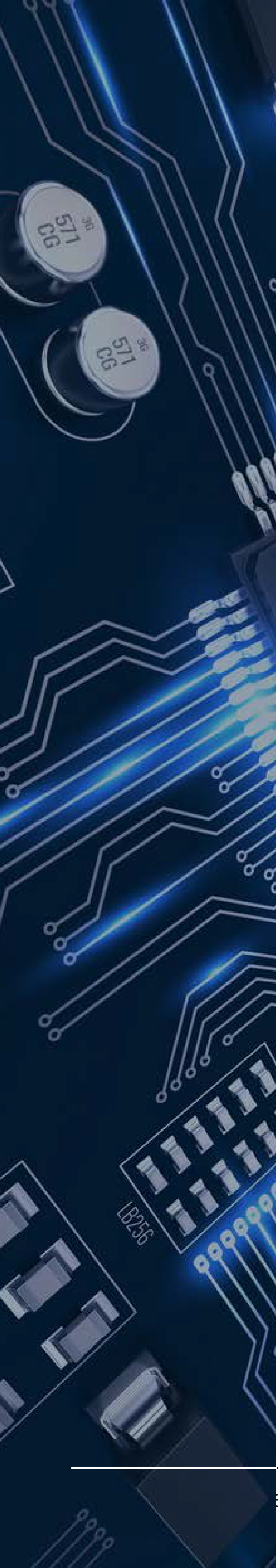
- Increase situational awareness for dismounted forces at lower echelons
- Lighten the physical load for dismounted forces
- Improve sustainment with automated ground resupply
- Facilitate movement with improved route clearance
- Protect the Force with EOD RAS platform and payload improvements

RAS in Action

Squads and platoons equipped with small RAS in urban terrain. They will use these systems to aid in reconnaissance missions across three dimensions (surface, supersurface, and subsurface) and to protect Soldiers.

Includes

- Squad Multipurpose Equipment Transports: Which carry supplies and small unit enablers, such as additional weapons, power generation, and other ground robots.
- Unmanned Aircraft System (UAS) sensors



MID-TERM (2021-2030)

The Army continues research in autonomy, machine learning, AI, power management, and common control to achieve more capable UGS and UAS.

Mid-Term Priorities

The primary focus is improvements in situational awareness, Soldier load reduction, sustainment and maneuver.

Strategies

- Increase situational awareness with advanced, smaller RAS and swarming
- Lighten the load with investments in new programs to pursue exoskeleton capabilities
- Improve sustainment with fully automated convoy operations
- Improve maneuver with unmanned combat vehicles and advanced payloads

Marines Test Next Generation Combat Systems

Click above to watch US Marines from 3rd Battalion, 5th Marine Regiment testing a variety of new warfighting technology - MAARS, MUUT, PD-100, Instant Eye. All of which aim to help the U.S. Army meets is goals.

FAR-TERM (2031-2040)

The Army fields new autonomous UGS and UAS developed through commercial research and science and technology investments made in the near- and mid-terms.

Far-Term Priorities

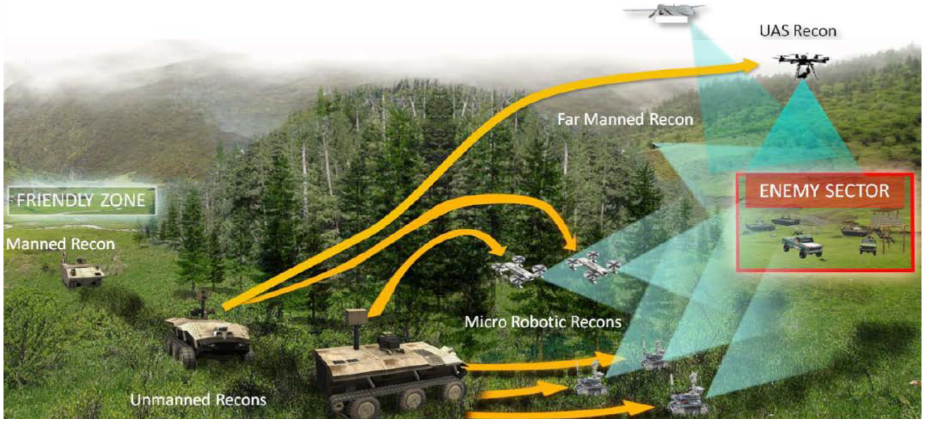
Allow Soldiers and leaders to focus on the execution of the mission rather than the manipulation and direct task control of robots. By fully integrating autonomous systems.

Strategies

- Increase situational awareness with persistent reconnaissance from swarming systems
- Improve sustainment with autonomous aerial cargo delivery
- Facilitate maneuver with advancements to unmanned combat vehicles

Unmanned Recon Scenario

Small UGS working alongside Soldiers with robotic integration across all formations and mission templates.



Includes

- Mounted scouts, augmented with vehicle-launched semi-autonomous Unmanned Aircraft System (UAS)
- Dismounted scouts, augmented with small ground robots

13TH
HOMELAND SECURITY WEEK

JOIN US IN WASHINGTON, D.C.

What HSW 2017 Will Deliver

350+ Attendees

10+ HOURS Reserved for Networking

20+ HOURS Reserved for Informational Content

The 13th Annual Homeland Security Week taking place October 22-24 will bring together top homeland security leaders from government, industry and academia alike to take a deep dive into current challenges and future requirements necessary for numerous government agencies, all directly or indirectly responsible for U.S. homeland security, to facilitate a complex, joint, multilayered plan to combat the evolving challenges our country faces.

LEARN MORE