EIB World Trade Headlines

Evolutions In Business • www.eib.com • (978) 256-0438
Fax: (978) 250-4529 • P.O. Box 4008. Chelmsford. MA 01824

March 1, 2016 - Volume 8, Issue 4

"Export Control Reform: Challenges for Small Business?"

Opening Remarks of Kevin J. Wolf Assistant Secretary of Commerce for Export Administration House Committee on Small Business Hearing

Thank you, Chairman Chabot and Ranking Member Velázquez. The purpose of export controls is to create an enforceable regulatory net over the export, reexport, and transfer by foreign and domestic persons of specific types of commodities, software, technology, and services to specific destinations, end uses, or end users for various national security, foreign policy, and other reasons. Unless those affected by the regulations understand them, they cannot comply with them, and the national security and foreign policy objectives of the controls will not be met. This is why outreach and education, particularly of small- and medium-sized companies, is a vital part of our mission. Hearings such as this and your continued interest in the topic help us considerably. So, thank you again.

As with most areas of regulation, export controls are inherently complex. Some items and activities warrant strict controls, many warrant few controls, and others warrant a mix depending on the circumstances of a particular transaction. Not all destinations, end uses, and end users are of equal concern. Foreign policy concerns and priorities change over time. Technologies evolve. Newly developed technologies can be extremely sensitive; others morph from predominant military use to something that is in normal commercial use. Controls are needed on end uses and end users of concern even if the items involved are widely available or unsophisticated. Subtle differences in fact patterns or technical characteristics of a product can have significantly different outcomes in the scope of control. Most controls reflect compromises in wording and scope reached by dozens of like-minded countries in multilateral export control arrangements.

*(*Continued On The Following Page)*

NEWSLETTER NOTES

All reflect consensus views of the law enforcement, national security, foreign policy, and economic security equities of multiple U.S. government agencies.

Finally, the controls are an aggregation of decades of individual statutory and regulatory decisions spread out over multiple government agencies written and edited by hundreds of different individuals that have accreted into the complex system we have today. In the abstract, there are, in the extreme, two ways to make the system vastly more simple -- require a license everywhere, all the time, always for all items or all listed items or don't require a license at all unless specifically informed by the government.
The former, of course, would impose a massive and devastating regulatory burden on exports and require the creation of a U.S. Government export control infrastructure far larger than what we have today. The latter would not satisfy the national security and foreign policy objectives of the controls. There is thus an inherent tension in export controls between simple, broad regulations that control too much and impose an excessive licensing burden, on the one hand, and tailored, detailed controls that control just the right amount but are initially more complex to work through, on the other. This is the daily challenge for export control policy makers -- deciding where the lines should be drawn. This Administration has focused on trying to tailor the controls to reduce the overall regulatory burden as much as possible without compromising the national security and foreign policy objectives of the controls. This means that education and outreach are vital to the success of the effort.

Although there are many U.S. government agencies that control the export of items in one form or another, the two agencies with the largest portion of the responsibility are represented here before you today -- the Commerce Department's Bureau of Industry and Security (BIS), which administers the Export Administration Regulations (EAR), and the State Department's Directorate of Defense Trade Controls (DDTC), which administers the International Traffic in Arms Regulations (ITAR). I can assure you that both BIS and DDTC management and staff are committed to administering their controls in the least burdensome way possible without impairing the national security and foreign policy objectives of the controls.

These are not just words. The Obama Administration launched in 2010 the most fundamental reform of the system since World War II. The reform focuses our controls on those items that must be rigorously protected while ensuring that our controls do not drive foreign customers to foreign suppliers and U.S. companies offshore. Two significant parts of this plan are nearly complete -- (1) the transfer of less sensitive military and commercial satellite items from the ITAR to the EAR to allow for more flexible controls over trade with allied countries and (2) the update and harmonization of key EAR and ITAR terms and principles to reduce inherent regulatory burdens.

*(*Continued On The Following Column)*

Once companies learn and adapt to the new structures -- and we recognize that the transition process can be difficult -- the regulatory compliance obligations, particularly for small and medium-sized companies, will generally be materially reduced.

First, the revisions identify more clearly what is actually controlled. For too long, determinations about what was and was not controlled, and which list governed an item, were, as a practical matter, more a function of lore rather than law. Over the last six years, we have engaged in a massive industry outreach effort to ask for help in rewriting most of the controls in ways that industry can better understand. Every change was proposed for comment -- some more than once -- to ensure that we got it as clear as possible. Second, the rebuilding of the control lists moved -- but did not de-control -- hundreds of thousands of items, mostly parts and components predominantly manufactured by small businesses, and related technologies from State's regulations to the more flexible Commerce regulations. The transfer to Commerce's regulations of these less sensitive military and commercial satellite and space items eliminates many regulatory burdens.

For example, for the items that have moved to the Commerce list from the State list:

• There are no registration requirements. This eliminates the expense of paying to register and the burden and expense of preparing and submitting these forms or fees. For those companies with a limited product line where all their items have transferred, this allows for a significant reduction in burden and cost.

• There are no fees for submitting license applications. For small companies exporting products with low margins, this is a significant advantage.

• There are no requirements to get permission merely to manufacture or to market abroad. The Commerce regulations, of course, still control the flow of goods, technology, and software, but with far shorter and simpler forms than State's Manufacturing License Agreements and Technical Assistance Agreements.
Most Commerce authorizations also have significantly fewer conditions and regulatory burden requirements than do State's agreements.

• There are no per se requirements to have a purchase order for each application. This means that an exporter can resolve its licensing obligations before knowing whether it has a sale, which saves time. It also dramatically reduces the total number of applications and licenses needed over the duration of a regular relationship with a foreign customer that will involve multiple purchase orders.

(*Continued On The Following Page)

• Except in situations involving military and satellite items destined to countries subject to embargoes, the Commerce rules generally do not have a "see through" rule. This is the rule that means that an item is always subject to U.S. jurisdiction even when incorporated into foreign-made items or uncontrolled items. For trade with non-embargoed countries, the Commerce regulations have a de minimis rule, which means that if the value of controlled US-origin content is less than 25%, then the foreign-made item is generally not subject to U.S. jurisdiction. This change largely eliminates the incentive for foreign companies in non-embargoed destinations to design-out U.S. origin items, particularly parts and components. It thus bolsters the health and competitiveness of the U.S. industrial base because those in non-embargoed countries will generally no longer need to second source parts and components elsewhere.

• Most importantly, the Commerce regulations have multiple license exceptions that do not exist in the State regulations, and which State is prohibited by law from creating. In most cases, these exceptions allow exporters to ship their products to allied and other non-embargoed countries without the need to apply to the government for a license, assuming the parties are willing to abide by various recordkeeping and other conditions to help ensure compliance with the exceptions. One of the exceptions developed as part of the reform effort, License Exception Strategic Trade Authorization (STA), allows for significant reductions in regulatory burdens associated with trade with NATO and other close allies. It enhances our national security by making our systems more interoperable.

For all these reasons and others, the Export Control Reform effort helps small businesses, particularly defense exporters, by increasing the security of supply from small companies that are the second and third tier suppliers in the defense industry, facilitating timely and reliable supplier relationships between U.S. exporters and their foreign customer base, and enhancing their long-term health and competitiveness. These sectors include aerospace, military vehicles, marine vessels, space, satellites, and electronics.

There are many other actions Commerce has taken to make compliance for small and medium-sized companies easier. For many years, the Departments of Commerce, State, and Treasury have maintained eleven separate lists of entities that are sanctioned for various national security and foreign policy reasons, including for illegally exporting arms or other items, violating US sanctions, engaging in terrorism, and trafficking narcotics. If a company or individual appears on the list, U.S. firms must do further research into the individual or company in accordance with the administering agency's rules before doing business with them. To ease this review process, an interagency task force created the Consolidated Screening List (CSL) in 2009 so that all eleven lists can be accessed in one place.

*(*Continued On The Following Column)*

Further, in July 2015, the Department of Commerce created a new web search tool to help US companies easily search the CSL. This CSL web search tool has "Fuzzy Name Search" capabilities enabling companies to search the CSL without knowing the exact spelling of an entity's name. This is particularly helpful when searching for names on the CSL that have been transliterated into English from non-Latin alphabet languages. All of these actions taken together have greatly benefitted U.S. companies by reducing the time needed to search all eleven lists and by providing a free alternative to costly third-party software vendors. We also revised a number of license exceptions, such as those for temporary exports, exports of replacement parts, and exports to governments in order to broaden their scope and to make them less burdensome. They still need work but they are better. We've increased the license validity periods and greatly expanded, as a matter of practice, the flexibility of our licenses so that they can be tailored to specific transactions. We revised and significantly reduced the support document requirements – requirements that were among the most complicated sections of the EAR. We have simplified the license conditions on approved licenses.

As evidence of how important education and outreach are to our bureau, I would like to give you some representative examples. In Fiscal Year 2015, we estimate that our outreach programs resulted in over 100,000 interactions with U.S. and foreign persons. We conducted over 350 events for industry, including the weekly teleconferences that I host on specific Export Control Reform topics, the seminars that are held throughout the country and overseas, the industry group meetings at which we speak, our Technical Advisory Committee meetings, the small- and medium-sized business conferences that we attend, and the webinars we produce. We conducted outreach events in 18 states and ten foreign countries. We've conducted or participated in 51 seminars in the United States.

Our seminars and online services are an effective way for small- and medium-sized exporters to understand their responsibilities as members of the regulated community. We have published several blog posts on the Commerce Department website on how export control reform benefits small businesses and entrepreneurs, and we worked with the Small Business Administration (SBA) to share this information through their social media networks. We have added over 6,700 new users to SNAP-R, our electronic license application system, bringing the total number of users to over 36,400. The online interactive decision tools we have developed received over 33,000 hits. The BIS website has additional tools and resources in our Exporter Portal. In addition, our Office of Exporter Services counseling line provides exporters with free counseling via telephone. Our export counseling staff has answered over 33,000 telephone and e-mail inquiries.

*(*Continued On The Following Page)*

We have partnered with SBA on a number of efforts. For example, BIS Under Secretary Eric Hirschhorn conducted a training session for SBA international trade staff from 68 district offices and 20 export assistance centers across the country. The training was designed to help SBA staff identify companies who may be covered by export control regulations and direct them to BIS resources. Through such sessions, BIS utilizes SBA's network to help inform small- and medium-sized businesses. BIS has also collaborated with SBA and other organizations representing the interests of small and medium-sized enterprises at a number of conferences. At our annual Update conference, we partnered with SBA, the National Small Business Association, the Maryland Small Business Development Center (MDSBDC), and the Minority Business Development Agency. In 2015, BIS sent outreach, regulatory policy, and compliance staff to the Association of Small Business Development Centers' (ASBDC) annual conference in San Francisco and counseled approximately 150 SBDC advisors. BIS representatives spoke at four programs sponsored by ASBDC in collaboration with the Bureau of the Census to educate exporters and freight forwarders on properly reporting required information in the Automated Export System. As a result of this partnership, ASBDC has increased the number of export control-related workshops and exhibitors at its annual conference, and begun to offer a certificate in international trade and related-regulations to its membership.

BIS has held open fora on SME comparative trade issues and participated in state-level trade conferences to facilitate trade. In 2015, the President's Export Council Subcommittee on Export Administration, one of BIS's industry advisory committees, prioritized its work with the National Institute of Standards and Technology's ExportTech program, a national export assistance program that targets small- and medium-sized businesses. BIS representatives participated in a webinar sponsored by FedEx that was intended to reach FedEx's small- and medium-sized exporting customers.
For this year, we plan to sponsor or co-sponsor 23 seminars, including the annual Update conference and the West Coast Export Control Forum, in thirteen different states. We will develop and conduct many new webinars and will post additional new educational videos on our website. BIS staff, including the Under Secretary and I, will continue attending as many compliance conferences and company training events as possible. I will also continue to answer, every Wednesday at 2:30 over an open, free conference call, every question that comes into BIS. These calls have been highly popular, particularly with small- and medium-sized companies, which generally do not have large legal teams or compliance staffs.

In addition to the short- and near-term rationalization benefits for small- and mediumsized companies, this work has established the framework for what could be an even more significant rationalization and simplification of the system,

*(*Continued On The Following Column)*

which is the creation of a common set of export control regulations and then, eventually, with the help of Congress, a single export licensing agency that would administer a single set of regulations with a single list of controlled items. In addition, now that the internal work on a common IT system for interagency review of Commerce license applications is almost complete, we're renewing the effort we started a few years ago to complete a common Internet-based license application portal for both Commerce and State and a single license application form common to both the EAR and the ITAR. We will need a lot of industry input and advice as we move to this next step to make sure it is modern and effective.

Additionally, under ECR, the President established the Federal Export Enforcement Coordination Center, to which the Commerce Department contributes several personnel. Among its mandates, the Center will coordinate law enforcement public outreach activities related to U.S. export controls. In the current U.S. export controls system, there are several federal regulatory (including Commerce's BIS and State's DDTC) and enforcement agencies (BIS' Office of Export Enforcement and U.S. Immigration and Customs Enforcement 's Homeland Security Investigations), involved in outreach to industry often targeting the same exporters or industry sectors, leading to confusion regarding proper reporting or disclosure to government agencies. Coordination of these efforts will result in a more seamless, efficient, and holistic U.S. government approach to private sector outreach to include small businesses.

In conclusion, the ECR goal of creating a new export control system defined by what we called the "Four Singularities" – a single control list, a single licensing agency (SLA), a single IT, and a primary export enforcement coordination agency was structured with the issues of small- and medium-sized companies in mind. We recognized that small firms account for more than 99 percent of all employers, 98 percent of all exporters, and a third of the annual value of U.S. exports. They are the engine of technological innovation and it is thus in our national and economic security interests to ensure that these small businesses can successfully navigate the nation's export control system. We understand that getting used to the new system can be a burden. This is why we have stretched the implementation of the changes out over a number of years, with significant delayed effective dates and multiple opportunities for industry to comment on the proposed rules years before they became effective. I am completely confident, however, that once the essence of the reform effort is in place and companies have adapted to it, it will properly implement the national security and foreign policy objectives of the controls in the least burdensome way possible. I look forward to your ideas, suggestions, and help for this part of our mission. Thank you.

(*Continued On The Following Page)

USS Bataan Completes Sea Trials

Amphibious assault ship USS Bataan (LHD 5) completed sea trials Feb. 1 after conducting major shipyard maintenance over the past 12 months.

Sea trials are conducted after ships complete major shipyard maintenance and tests the ship's systems and to make sure the ship is ready for deployment.

"Sea trials provided the ship with a series of tests and validations in order to test newly installed, modified or overhauled equipment," said Chief Warrant Officer 3 Aaron Dowdy from Richmond, Virginia, the ship's repair officer. "Major equipment that needed testing included radars, the ship's propulsion system and the countermeasure wash down system, which is designed to defend the ship against chemical, biological and radiological attack."

Thanks to cooperation between Bataan Sailors and shipyard workers, work was performed to further prepare the ship to answer the nation's call.

"Sea trial success comes from Sailors and shipyard workers quickly learning how to work together," Dowdy said. "It's been months of planning and training. When it came down to execution, the crew was ready, and they made it happen."

Bataan's crew has been working many months in preparation for sea trials. The ship's maintenance period started in February 2015 in BAE Shipyards with the ship going into drydock. The crew spent months prior to that identifying maintenance needs and requesting them through the ship's maintenance system. After months of hard work from the crew and the shipyard workers, the ship returned to Naval Station Norfolk in December. Now all their hard work has paid off.

"The necessary system checks and work by the crew during sea trials makes certain Bataan will be ready to rejoin the fleet and get the crew for their next deployment," said Dowdy. "After a long shipyard period, it feels great to get the ship back out to sea. I'm extremely happy with the way the crew has come together and performed."

*(*Continued On The Following Column)*

Bataan's crew has been working many months in preparation for sea trials. The ship's maintenance period started in February 2015 in BAE Shipyards with the ship going into drydock. The crew spent months prior to that identifying maintenance needs and requesting them through the ship's maintenance system. After months of hard work from the crew and the shipyard workers, the ship returned to Naval Station Norfolk in December. Now all their hard work has paid off.

"The necessary system checks and work by the crew during sea trials makes certain Bataan will be ready to rejoin the fleet and get the crew for their next deployment," said Dowdy. "After a long shipyard period, it feels great to get the ship back out to sea. I'm extremely happy with the way the crew has come together and performed."

Once sea trials are completed, the ship will begin its training and qualification cycle. Sailors, new and old, will train and then be tested to show they are ready for the ship's next deployment.

"Since returning from deployment in 2014, we set three priorities here aboard Bataan," said Bataan's Commanding Officer Capt. John "JC" Carter. "Our first two priorities were taking care of the Sailor and taking care of the Bataan family. After a long deployment, these were at the top of the list."

"Our third priority was taking care of the ship," said Carter. "This crew, along with quite a number of new Sailors who checked into the command this past year, have stepped up to the plate and seriously hit a home run. I couldn't be prouder of the accomplishments we've made during this maintenance period."

Bataan is scheduled to begin the basic phase of the Optimized Fleet Response Training Plan in order to prepare for future deployments.

Cybersecurity National Action Plan

Taking bold actions to protect Americans in today's digital world.

*(*Continued On The Following Page)*

From the beginning of his Administration, the President has made it clear that cybersecurity is one of the most important challenges we face as a Nation, and for more than seven years he has acted comprehensively to confront that challenge. Working together with Congress, we took another step forward in this effort in December with the passage of the Cybersecurity Act of 2015, which provides important tools necessary to strengthen the Nation's cybersecurity, particularly by making it easier for private companies to share cyber threat information with each other and the Government.

But the President believes that more must be done – so that citizens have the tools they need to protect themselves, companies can defend their operations and information, and the Government does its part to protect the American people and the information they entrust to us. That is why, today, the President is directing his Administration to implement a **Cybersecurity National Action Plan (CNAP)** that takes near-term actions and puts in place a long-term strategy to enhance cybersecurity awareness and protections, protect privacy, maintain public safety as well as economic and national security, and empower Americans to take better control of their digital security.

The Challenge

From buying products to running businesses to finding directions to communicating with the people we love, an online world has fundamentally reshaped our daily lives. But just as the continually evolving digital age presents boundless opportunities for our economy, our businesses, and our people, it also presents a new generation of threats that we must adapt to meet. Criminals, terrorists, and countries who wish to do us harm have all realized that attacking us online is often easier than attacking us in person. As more and more sensitive data is stored online, the consequences of those attacks grow more significant each year. Identity theft is now the fastest growing crime in America. Our innovators and entrepreneurs have reinforced our global leadership and grown our economy, but with each new story of a high-profile company hacked or a neighbor defrauded, more Americans are left to wonder whether technology's benefits could risk being outpaced by its costs.

The President believes that meeting these new threats is necessary and within our grasp. But it requires a bold reassessment of the way we approach security in the digital age. If we're going to be connected, we need to be protected. We need to join together—Government, businesses, and individuals—to sustain the spirit that has always made America great.

*(*Continued On The Following Column)*

Our Approach

That is why, today, the Administration is announcing a series of near-term actions to enhance cybersecurity capabilities within the Federal Government and across the country. But given the complexity and seriousness of the issue, the President is also asking some of our Nation's top strategic, business, and technical thinkers from outside of government to study and report on what more we can do to enhance cybersecurity awareness and protections, protect privacy, maintain public safety as well as economic and national security, and empower Americans to take better control of their digital security. Bold action is required to secure our digital society and keep America competitive in the global digital economy.>/p>

The President's **Cybersecurity National Action Plan (CNAP)** is the capstone of more than seven years of determined effort by this Administration, building upon lessons learned from cybersecurity trends, threats, and intrusions. This plan directs the Federal Government to take new action now and fosters the conditions required for long-term improvements in our approach to cybersecurity across the Federal Government, the private sector, and our personal lives. Highlights of the CNAP include actions to:

***Establish the "Commission on Enhancing National Cybersecurity."** This Commission will be comprised of top strategic, business, and technical thinkers from outside of Government – including members to be designated by the bi-partisan Congressional leadership. The Commission will make recommendations on actions that can be taken over the next decade to strengthen cybersecurity in both the public and private sectors while protecting privacy; maintaining public safety and economic and national security; fostering discovery and development of new technical solutions; and bolstering partnerships between Federal, State, and local government and the private sector in the development, promotion and use of cybersecurity technologies, policies, and best practices.

*Modernize Government IT and transform how the Government manages cybersecurity through the proposal of a **$3.1 billion Information Technology Modernization Fund**, which will enable the retirement, replacement, and modernization of legacy IT that is difficult to secure and expensive to maintain, as well as the formation of a new position – the **Federal Chief Information Security Officer** – to drive these changes across the Government.

*(*Continued On The Following Page)*

***Empower Americans to secure their online accounts** by moving beyond just passwords and adding an extra layer of security. By judiciously combining a strong password with additional factors, such as a fingerprint or a single use code delivered in a text message, Americans can make their accounts even more secure. This focus on **multi-factor authentication** will be central to a new **National Cybersecurity Awareness Campaign** launched by the **National Cyber Security Alliance** designed to arm consumers with simple and actionable information to protect themselves in an increasingly digital world. The National Cyber Security Alliance will partner with leading technology firms like **Google**, **Facebook**, **DropBox**, and **Microsoft** to make it easier for millions of users to secure their online accounts, and financial services companies such as**MasterCard**, **Visa**, **PayPa**l, and **Venmo** that are making transactions more secure. In addition, the Federal Government will take steps to safeguard personal data in online transactions between citizens and the government, including through a **new action plan** to drive the Federal Government's adoption and use of effective identity proofing and strong multi-factor authentication methods and a systematic review of where the Federal Government can reduce reliance on Social Security Numbers as an identifier of citizens.

***Invest over $19 billion for cybersecurity as part of the President's Fiscal Year (FY) 2017 Budget**. This represents a more than 35 percent increase from FY 2016 in overall Federal resources for cybersecurity, a necessary investment to secure our Nation in the future.

Through these actions, additional new steps outlined below, and other policy efforts spread across the Federal Government, the Administration has charted a course to enhance our long-term security and reinforce American leadership in developing the technologies that power the digital world.

Commission on Enhancing National Cybersecurity

For over four decades, computer technology and the Internet have provided a strategic advantage to the United States, its citizens, and its allies. But if fundamental cybersecurity and identity issues are not addressed, America's reliance on digital infrastructure risks becoming a source of strategic liability. To address these issues, we must diagnose and address the causes of cyber-vulnerabilities, and not just treat the symptoms. Meeting this challenge will require a long-term, national commitment.

*(*Continued On The Following Column)*

To conduct this review, the President is establishing the **Commission on Enhancing National Cybersecurity**, comprised of top strategic, business, and technical thinkers from outside of Government – including members to be designated by the bi-partisan Congressional leadership. The Commission is tasked with making detailed recommendations on actions that can be taken over the next decade to enhance cybersecurity awareness and protections throughout the private sector and at all levels of Government, to protect privacy, to maintain public safety and economic and national security, and to empower Americans to take better control of their digital security. The National Institute of Standards and Technology will provide the Commission with support to allow it to carry out its mission. The Commission will report to the President with its specific findings and recommendations before the end of 2016, providing the country a roadmap for future actions that will build on the CNAP and protect our long-term security online.

Raise the Level of Cybersecurity across the Country

While the Commission conducts this forward looking review, we will continue to raise the level of cybersecurity across the Nation.

Strengthen Federal Cybersecurity The Federal Government has made significant progress in improving its cybersecurity capabilities, but more work remains. To expand on that progress and address the longstanding, systemic challenges in Federal cybersecurity, we must re-examine our Government's legacy approach to cybersecurity and information technology, which requires each agency to build and defend its own networks. These actions build upon the foundation laid by the **Cybersecurity Cross-Agency Priority Goals** and the **2015 Cybersecurity Strategy and Implementation Plan**.

*The President's 2017 Budget proposes a **$3.1 billion Information Technology Modernization Fund**, as a down payment on the comprehensive overhaul that must be undertaken in the coming years. This revolving fund will enable agencies to invest money up front and realize the return over time by retiring, replacing, or modernizing antiquated IT infrastructure, networks, and systems that are expensive to maintain, provide poor functionality, and are difficult to secure.

*The Administration has created the position of **Federal Chief Information Security Officer** to drive cybersecurity policy, planning, and implementation across the Federal Government. This is the first time that there will be a dedicated senior official who is solely focused on developing, managing, and coordinating cybersecurity strategy, policy, and operations across the entire Federal domain.

*(*Continued On The Following Page)*

*The Administration is requiring agencies to identify and prioritize their **highest value and most at-risk IT assets** and then take additional concrete steps to improve their security.

*The Department of Homeland Security, the General Services Administration, and other Federal agencies will increase the availability of **government-wide shared services for IT and cybersecurity**, with the goal of taking each individual agency out of the business of building, owning, and operating their own IT when more efficient, effective, and secure options are available, as well as ensuring that individual agencies are not left on their own to defend themselves against the most sophisticated threats.

*The Department of Homeland Security is **enhancing Federal cybersecurity by expanding the EINSTEIN and Continuous Diagnostics and Mitigation programs**. The President's 2017 Budget supports all Federal civilian agencies adopting these capabilities.

*The Department of Homeland Security is dramatically **increasing the number of Federal civilian cyber defense teams to a total of 48**, by recruiting the best cybersecurity talent from across the Federal Government and private sector. These standing teams will protect networks, systems, and data across the entire Federal Civilian Government by conducting penetration testing and proactively hunting for intruders, as well as providing incident response and security engineering expertise.

*The Federal Government, through efforts such as the National Initiative for Cybersecurity Education, will enhance cybersecurity education and training nationwide and hire more cybersecurity experts to secure Federal agencies. As part of the CNAP, the President's Budget invests **$62 million in cybersecurity personnel** to:

*Expand the Scholarship for Service program by establishing a **CyberCorps Reserve** program, which will offer scholarships for Americans who wish to obtain cybersecurity education and serve their country in the civilian Federal government;

*Develop a **Cybersecurity Core Curriculum** that will ensure cybersecurity graduates who wish to join the Federal Government have the requisite knowledge and skills; and,

*Strengthen the **National Centers for Academic Excellence in Cybersecurity Program** to increase the number of participating academic institutions and students, better support those institutions currently participating, increase the number of students studying cybersecurity at those institutions, and enhance student knowledge through program and curriculum evolution.

*(*Continued On The Following Column)*

*The President's Budget takes additional steps to expand the cybersecurity workforce by:

*Enhancing **student loan forgiveness programs for cybersecurity experts** joining the Federal workforce;

*Catalyzing investment in cybersecurity education as part of a robust computer science curriculum through **the President's Computer Science for All Initiative**.

Empower Individuals The privacy and security of all Americans online in their daily lives is increasingly integral to our national security and our economy. The following new actions build on the President's **2014 BuySecure Initiative** to strengthen the security of consumer data.

*The President is calling on Americans to move beyond just the password to leverage **multiple factors of authentication** when logging-in to online accounts. Private companies, non-profits, and the Federal Government are working together to help more Americans stay safe online through a new public awareness campaign that focuses on broad adoption of multi-factor authentication. Building off the Stop.Think.Connect. campaign and efforts stemming from the National Strategy for Trusted Identities in Cyberspace, the National Cyber Security Alliance will **partner with leading technology companies and civil society** to promote this effort and make it easier for millions of users to secure their accounts online. This will support a broader effort to increase public awareness of the individual's role in cybersecurity.

*The Federal Government is **accelerating adoption of strong multi-factor authentication and identity proofing** for citizen-facing Federal Government digital services. The General Services Administration will establish a new program that will better protect and secure the data and personal information of Americans as they interact with Federal Government services, including tax data and benefit information.

*The Administration is conducting a systematic review of where the Federal Government can **reduce its use of Social Security Numbers** as an identifier of citizens.

*The Federal Trade Commission recently relaunched **IdentityTheft.Gov**, to serve as a one-stop resource for victims to report identity theft, create a personal recovery plan, and print pre-filled letters and forms to send to credit bureaus, businesses, and debt collectors.

*The Small Business Administration (SBA), partnering with the Federal Trade Commission, the National Institute of Standards and Technology (NIST), and the Department of Energy, will offer **cybersecurity training to reach over 1.4 million small businesses** and small business stakeholders through 68 SBA District Offices, 9 NIST Manufacturing Extension Partnership Centers, and other regional networks across the country.

*(*Continued On The Following Page)*

*The Administration is announcing new milestones in **the President's BuySecure Initiative** to secure financial transactions. As of today the Federal Government has supplied over **2.5 million more secure Chip-and-PIN payment cards**, and transitioned to this new technology the entire fleet of card readers managed by the Department of the Treasury. Through government and private-sector leadership, more secure chip cards have been issued in the United States than any other country in the world.

Enhance Critical Infrastructure Security and Resilience The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure. A continued partnership with the owners and operators of critical infrastructure will improve cybersecurity and enhance the Nation's resiliency. This work builds off the President's previous cybersecurity focused Executive Orders on **Critical Infrastructure** (2013) and **Information Sharing** (2015).

*The Administration is announcing new milestones in **the President's BuySecure Initiative** to secure financial transactions. As of today the Federal Government has supplied over **2.5 million more secure Chip-and-PIN payment cards**, and transitioned to this new technology the entire fleet of card readers managed by the Department of the Treasury. Through government and private-sector leadership, more secure chip cards have been issued in the United States than any other country in the world.

Enhance Critical Infrastructure Security and Resilience The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure. A continued partnership with the owners and operators of critical infrastructure will improve cybersecurity and enhance the Nation's resiliency. This work builds off the President's previous cybersecurity focused Executive Orders on **Critical Infrastructure** (2013) and **Information Sharing** (2015).

*The Department of Homeland Security, the Department of Commerce, and the Department of Energy are contributing resources and capabilities to establish a **National Center for Cybersecurity Resilience** where companies and sector-wide organizations can test the security of systems in a contained environment, such as by subjecting a replica electric grid to cyber-attack.

*The Department of Homeland Security will **double the number of cybersecurity advisors** available to assist private sector organizations with in-person, customized cybersecurity assessments and implementation of best practices.

*(*Continued On The Following Column)*

*The Department of Homeland Security is collaborating with UL and other industry partners to develop a **Cybersecurity Assurance Program** to test and certify networked devices within the "Internet of Things," whether they be refrigerators or medical infusion pumps, so that when you buy a new product, you can be sure that it has been certified to meet security standards.

*The National Institute of Standards and Technology is **soliciting feedback** in order to inform further development of its **Cybersecurity Framework** for improving critical infrastructure cybersecurity. This follows two years of adoption by organizations across the country and around the world.

*Yesterday, Commerce Secretary Pritzker cut the ribbon on the new **National Cybersecurity Center of Excellence**, a public-private research and development partnership that will allow industry and government to work together to develop and deploy technical solutions for high-priority cybersecurity challenges and share those findings for the benefit of the broader community.

*The Administration is calling on major health insurers and healthcare stakeholders to help them take new and significant steps to enhance their data stewardship practices and ensure that consumers can trust that their sensitive health data will be safe, secure, and available to guide clinical decision-making.

Secure Technology Even as we work to improve our defenses today, we know the Nation must aggressively invest in the science, technology, tools, and infrastructure of the future to ensure that they are engineered with sustainable security in mind.

*Today the Administration is releasing its **2016 Federal Cybersecurity Research and Development Strategic Plan**. This plan, which was called for in the 2014 Cybersecurity Enhancement Act, lays out strategic research and development goals for the Nation to advance cybersecurity technologies driven by the scientific evidence of efficacy and efficiency.

*In addition, the Government will work with organizations such as the Linux Foundation's **Core Infrastructure Initiative** to fund and secure commonly used internet "utilities" such as open-source software, protocols, and standards. Just as our roads and bridges need regular repair and upkeep, so do the technical linkages that allow the information superhighway to flow.

*(*Continued On The Following Page)*

Deter, Discourage, and Disrupt Malicious Activity in Cyberspace

Better securing our own digital infrastructure is only part of the solution. We must lead the international effort in adopting principles of responsible state behavior, even while we take steps to deter and disrupt malicious activity. We cannot pursue these goals alone – we must pursue them in concert with our allies and partners around the world.

*In 2015, members of the G20 joined with the United States in affirming important norms, including the applicability of international law to cyberspace, the idea that states should not conduct the cyber-enabled theft of intellectual property for commercial gain, and in welcoming the report of a United Nations Group of Governmental Experts, which included a number of additional norms to promote international cooperation, prevent attacks on civilian critical infrastructure, and support computer emergency response teams providing reconstitution and mitigation services. The Administration intends to institutionalize and implement these norms through **further bilateral and multilateral commitments** and confidence building measures.

*The Department of Justice, including the Federal Bureau of Investigation, is**increasing funding for cybersecurity-related activities by more than 23 percent** to improve their capabilities to identify, disrupt, and apprehend malicious cyber actors.

*U.S. Cyber Command is building a **Cyber Mission Force** of 133 teams assembled from 6,200 military, civilian, and contractor support personnel from across the military departments and defense components. The Cyber Mission Force, which will be fully operational in 2018, is already employing capabilities in support of U.S. Government objectives across the spectrum of cyber operations.

Improve Cyber Incident Response

Even as we focus on preventing and deterring malicious cyber activity, we must also maintain resilience as events occur. Over the past year, the country faced a wide array of intrusions, ranging from criminal activity to cyber espionage. By applying lessons learned from past incidents we can improve management of future cyber incidents and enhance the country's cyber-resilience.

*By this spring, the Administration will publicly release **a policy for national cyber incident coordination** and an accompanying **severity methodology** for evaluating cyber incidents so that government agencies and the private sector can communicate effectively and provide an appropriate and consistent level of response.

*(*Continued On The Following Column)*

Protect the Privacy of Individuals

In coordination with the information technology and cybersecurity efforts above, the Administration has launched a groundbreaking effort to enhance how agencies across the Federal Government protect the privacy of individuals and their information. Privacy has been core to our Nation from its inception, and in today's digital age safeguarding privacy is more critical than ever.

*Today, the President signed an Executive Order that created a permanent **Federal Privacy Council,** which will bring together the privacy officials from across the Government to help ensure the implementation of more strategic and comprehensive Federal privacy guidelines. Like cyber security, privacy must be effectively and continuously addressed as our nation embraces new technologies, promotes innovation, reaps the benefits of big data and defends against evolving threats.

Fund Cybersecurity

*In order to implement these sweeping changes, the Federal Government will need to invest additional resources in its cybersecurity. That is why the 2017 Budget allocates more than $19 billion for cybersecurity – a more than 35 percent increase over the 2016 enacted level. These resources will enable agencies to raise their level of cybersecurity, help private sector organizations and individuals better protect themselves, disrupt and deter adversary activity, and respond more effectively to incidents.

Upcoming BIS Seminars in Pittsburgh, PA

The Bureau of Industry and Security invites you to register for these upcoming seminars to learn about export control requirements under the Export Administration Regulations.
Essentials of U.S. Export Controls - 1 Day March 16, 2016
Pittsburgh, PA Registration: $275

This is an intensive, one-day program that covers the key information you need to know to comply with the Export Administration Regulations (EAR). Counseling and other professionals from the Bureau of Industry and Security will cover the major elements of the U.S. export control system for commercial exports. This fast-paced program is ideal for those with busy schedules.

*(*Continued On The Following Page)*

For information and registration go to: http://www.bis.doc.gov/index.php/compliance-a-training/current-seminar-schedule/81-compliance-a-training/export-administration-regulations-training/seminar-details/972-march-16-2016-pittsburgh-pa

How to Develop an Export Management and Compliance Program - 1 Day March 17, 2016 Pittsburgh, PA Registration: $275 Developing and maintaining an export management and compliance program is highly recommended to ensure that export transactions comply with the Export Administration Regulations (EAR), and to prevent export control violations. This one-day workshop provides an overview of the steps a company may take to implement an internal Export Management and Compliance Program. Agenda topics include guidance on how to establish an EMCP; strategies to improve your company's compliance program; how to avoid common compliance errors; and how to build a solid framework for your company's compliance program. This program includes small group discussion, hands-on exercises, one-on-one counseling opportunities, and compliance peer networking.

This program will be led by senior export compliance specialists from the Bureau of Industry and Security. Note: The information presented in this program is not a legal requirement of the Export Administration Regulations. It is intended to give informational advice and guidance based on industry best practices in the field of compliance. Recommended prerequisite: Essentials of Export Controls or Complying with U.S. Export Controls or equivalent experience.

For information and registration go to:http://www.bis.doc.gov/index.php/compliance-a-training/current-seminar-schedule/81-compliance-a-training/export-administration-regulations-training/seminar-details/973-march-17-2016-pittsburgh-pa

For general information about the BIS Seminar Program contact the Outreach and Educational Services Division at, OESDSeminar@bis.doc.gov. or 202/482-6031.

Aerospace Giants Honeywell, United Technologies Discussing Merger Again, Report Says

Honeywell has reportedly revived talks with rival United Technologies about a blockbuster deal that would create an aerospace colossus. Above, a visitor takes a closer look at a Honeywell aircraft engine displayed at the Asian Aerospace 2006 show in Singapore Feb. 22, 2006.

*(*Continued On The Following Column)*

UPDATE 7 p.m. EST: United Technologies Corp. rejected Honeywell's recent bid to merge, citing antitrust concerns, the Wall Street Journal reported.

Original story:

Honeywell International Inc. is in merger talks with United Technologies Corp. that could create an aerospace giant with annual sales of around $90 billion, according to anonymous sources who spoke to CNBC Monday. Discussions occurred this month with Honeywell offering mostly stock for its rival, the report said.

There is no assurance these talks will result in a deal, and some involved in the negotiations on the United Technologies side have expressed concerns the combination could face antitrust issues. Any agreement would be larger than the estimated $68.6 billion deal bringing together the American industrial behemoths Dow Chemical Co. and DuPont that was announced late last year.

Honeywell and United Technologies make many of the systems that go into commercial and military aircraft, so their proposed combination likely would face opposition from Airbus Group SE and Boeing Co.

Honeywell and United Technologies have been in talks off and on for much of the past year, but disagreements over which company would control the combined entity has stymied progress. In 2000, United Technologies was outbid by General Electric Co. in an attempt to take over Honeywell, but European antitrust regulators blocked the transaction.

GKN Aerospace 2015 net profit gains almost 17%

LONDON--British aerospace and automotive equipment supplier GKN PLC on Tuesday reported a 16.6% rise in profit for 2015, driven by a slight recovery in global light vehicle sales and continued strength in commercial aerospace.

Net profit rose to 197 million pounds ($277.9 million) from GBP169 million in the previous year, the Redditch, England-based company said. Profit also benefited from some exchange-rate accounting adjustments.

Sales grew 4% to GBP7.2 billion.

GKN has been deepening its involvement in the growing commercial aerospace market and last year acquired Fokker Technologies to add new structures and plane-wiring capacity.

The integration of the business is proceeding well, GKN said. The unit added GBP113 million in sales, though it also came with GBP18 million in restructuring costs for measures the company had embarked upon before GKN's purchase of Fokker. Another GBP35 million in restructuring costs are planned this year, GKN said.

"We expect 2016 to be a year of good growth, helped by the contribution from Fokker," Chief Executive Nigel Stein said.

Aerospace sales this year are expected to be broadly flat, the company said, with growth expected in the car-related driveline and metallurgy units. Land systems, which supply the agriculture market, is expected to continue to struggle with a drop in sales next year again after a 10% fall in 2015, GKN said.

Write to Robert Wall at robert.wall@wsj.com

4 companies that have embraced the Internet of Things

Two years from now, it's estimated the number of devices making up the Internet of Everything will surpass 23 billion. To put that into perspective, that means the number of interconnected gadgets will outnumber the world's population 2.5 to 1.

The type of technologies that will make up this new sector will by and large already be well established, including things like smartphones, tablets, and computers, as well as wearables, TVs, and cars.

*(*Continued On The Following Column)*

With such a wide range of technology types making up the expanding world of IoT, a number of companies are beginning to set in place processes and business models to support the customer's needs and desires. A few have already done this, and to no one's surprise, their names are a who's who of industry leaders.

Texas Instruments
Upon analyzing the industry's needs, TI went ahead and set up hardware / software support for companies looking to develop applications within one of what the company views as being the six key markets for IoT: building and home automation, smart cities, smart manufacturing, wearables, health care, and automotive. Among the products offered: analog signal chain, power management, sensing, wireless connectivity, processors, and MCU.
To learn more, visit the TI IoT support center.

Vishay
In recent years, Vishay has made a concerted effort to really expand its product line to better accommodate the engineers and designers working on IoT applications; specifically, the company has focused on developing more passive and active solutions.

Among the areas of IoT that Vishay provides solutions for are wearable devices for things like biometric monitoring, devices either clipped on or carried in one's pocket, fitbands, patient monitoring, smart watches and smart glasses. Also, the company has expanded its product line to cover IoT technologies in the home; specifically, smart meters, lighting control, air conditioners, washing machines, induction cooking, refrigerators and freezers, and robotic vacuum cleaners.

To learn more, visit the Vishay IoT education center.

*(*Continued On The Following Page)*

Digi-Key
Digi-Key, meanwhile, has really focused its efforts on wireless control; specifically, supporting the discrete controllers and transceivers that engineers can use to better create a low-cost, tightly-integrated design. The company believes that by pairing the right products with IoT designers, the amount of time spent designing these solutions can be reduced, and neither space nor performance is compromised.

To learn more about Digi-Key's approach to supporting today's IoT engineers and designers, head to the company's site.

Mouser
The thought leaders at Mouser believe that the IoT comes down to one very simple viewpoint: it's all about interconnecting wireless connectivity and sensors. A bit more specifically, the multiple connected embedded systems within an IoT network are really just independent microcontroller-based computers outfitted with sensors for the purpose of collecting and relaying data over a wireless protocol like WiFi, Bluetooth, or some other custom communication system.

It's an interesting concept that is further expounded upon when considering how best to protect this information with data encryption. To learn more about the company's view on this specific matter, visit Mouser.com

The CBRN Defence Sector is Set to Be Worth $11,275m in 2016, According to a New Study on ASDReports

The report, now available on ASDReports, CBRN Defence Market Report 2016-2026: Analysis of Top Companies & Forecasts of Chemical, Biological, Radiological & Nuclear Detection, Protection, Decontamination, Simulation & Training Equipment report indicates that the CBRN defence sector is set to be worth $11,275m in 2016 due to the current international geopolitical scenarios and the increasing technical sophistication of the technology involved.

Alessandra Giovanzanti, the defence analyst and the author of CBRN defence report commented that:

"The use of chemical weapons by the Assad regime in Syria as well as by Daesh in the Levant, incidents in nuclear plants such as the Fukushima disaster of 2011, the Ebola crisis, and the phenomenon of antibiotic resistant bacteria and viruses, all have drawn renewed attention upon the importance of CBRN defence for the protection of military and first responders in the field, as well as first line of protection for critical infrastructures and the civilian population."

*(*Continued On The Following Column)*

The 424 page report contains 348 tables, charts and graphs that utilise visual representation in order to clarify trends and market projections within the CBRN defence market. Visiongain provides a range of forecasts for the period 2016-2026 as well as for four submarket sectors: Detection, Protection, Decontamination, Simulation & Training.

In addition, nine leading national markets are analysed by visiongain over the period 2016-2026 while the 'Rest of the World' market includes unprecedented qualitative analysis of a further four national markets. The report also provides details of 350 CBRN contracts revealing where and with which technologies companies are achieving sales.

The report also provides profiles of 20 leading companies operating within the market and includes three exclusive expert interviews with: William F. Hesse, Military & Civil Defence Business Development Manager - Americas, Scott Safety; Ahti Luukkonen, Vice President, Sales & Marketing, Environics OY; James Milnes - Director, Hasta (UK) Ltd

Web Notice: Federal Register Notice 6797

Amendment to the International Traffic in Arms Regulations: U.S. Munitions List Categories VIII and XIX has been published and posted to the DDTC website. Click here to read Click here to read. (2.10.16)

http://www.pmddtc.state.gov/FR/2016/81FR02587.pdf

NOTE: In accordance with Title 17 U.S.C. Section 107, this material is distributed without profit or payment for non-profit news reporting and educational purposes only.