[H.A.S.C. No. 114–12]

HEARING

ON

NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2016

AND

OVERSIGHT OF PREVIOUSLY AUTHORIZED PROGRAMS

BEFORE THE

COMMITTEE ON ARMED SERVICES
HOUSE OF REPRESENTATIVES
ONE HUNDRED FOURTEENTH CONGRESS

FIRST SESSION

SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES HEARING

ON

INFORMATION TECHNOLOGY INVESTMENTS AND PROGRAMS: SUPPORTING CURRENT OPERATIONS AND PLANNING FOR THE FUTURE THREAT ENVIRONMENT

HEARING HELD
FEBRUARY 25, 2015

U.S. GOVERNMENT PUBLISHING OFFICE
94–099 WASHINGTON : 2015

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

JOE WILSON, South Carolina, *Chairman*

JOHN KLINE, Minnesota
BILL SHUSTER, Pennsylvania
DUNCAN HUNTER, California
RICHARD B. NUGENT, Florida
RYAN K. ZINKE, Montana
TRENT FRANKS, Arizona, *Vice Chair*
DOUG LAMBORN, Colorado
MO BROOKS, Alabama
BRADLEY BYRNE, Alabama
ELISE M. STEFANIK, New York

JAMES R. LANGEVIN, Rhode Island
JIM COOPER, Tennessee
JOHN GARAMENDI, California
JOAQUIN CASTRO, Texas
MARC A. VEASEY, Texas
DONALD NORCROSS, New Jersey
BRAD ASHFORD, Nebraska
PETE AGUILAR, California

KEVIN GATES, *Professional Staff Member*
LINDSAY KAVANAUGH, *Professional Staff Member*
JULIE HERBERT, *Clerk*

CONTENTS

INFORMATION TECHNOLOGY INVESTMENTS AND PROGRAMS: SUPPORTING CURRENT OPERATIONS AND PLANNING FOR THE FUTURE THREAT ENVIRONMENT

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ARMED SERVICES,
SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES,
Washington, DC, Wednesday, February 25, 2015.

The subcommittee met, pursuant to call, at 4:11 p.m., in room 2118, Rayburn House Office Building, Hon. Joe Wilson (chairman of the subcommittee) presiding.

OPENING STATEMENT OF HON. JOE WILSON, A REPRESENTATIVE FROM SOUTH CAROLINA, CHAIRMAN, SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

Mr. WILSON. Ladies and gentlemen, I call this hearing of the Emerging Threats and Capabilities Subcommittee to order. I am pleased to welcome everyone here today for the hearing on the fiscal year 2016 budget request for information technology [IT] programs for the Department of Defense [DOD].

Information technology systems are critical enablers for our military, enhancing the performance of individuals and units by connecting people and weapon systems together in ways that make them more effective than the sum of their parts. As we look at the budget request, and as the witnesses describe their relevant portions, I would like to ask each of you to address the following questions.

What systems are we investing in? How do these systems enhance the Department of Defense's ability to execute its missions, carry out business operations, and generally improve our ability to conduct warfighting operations? How do we prevent duplication between the services and agencies to make sure that the programs we pursue are deployed on time, on budget, and with the performance capabilities we originally planned?

Today we have invited a panel of dedicated public servants to answer these questions. Our witnesses are, first, the Honorable Terry Halvorsen, acting Chief Information Officer of the Department of Defense; Lieutenant General Robert S. Ferrell, Chief Information Officer/G–6 of the United States Army; Lieutenant General William J. Bender, Chief of Information Dominance and Chief Information Officer of the United States Air Force; Dr. John Zangardi, the acting Department of Navy Chief Information Officer, Deputy Assistant Secretary of the Navy for Command, Control, Communications, Computers, Intelligence, Information Operations and Space—quite a title; Brigadier General Kevin J. Nally, Director of

Command, Control, Communications and Computers (C4), the Chief Information Officer of the Marine Corps.

We also know that the Navy would like to submit additional testimony for the record for Vice Admiral Ted Branch, the Deputy Chief of Naval Operations for Information Dominance, who was unable to join us today.

If there are no objections, we will include that in the record.

[The statement of Admiral Branch can be found in the Appendix on page 87.]

Mr. WILSON. I would like to turn now to my friend, Mr. James Langevin of Rhode Island, the ranking member, for any comments he would like to make.

STATEMENT OF HON. JAMES R. LANGEVIN, A REPRESENTATIVE FROM RHODE ISLAND, RANKING MEMBER, SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

Mr. LANGEVIN. Thank you, Mr. Chairman.

And I want to thank Mr. Halvorsen, General Ferrell, General Bender, and Dr. Zangardi, and also General Nally. Thank you all for appearing before the subcommittee today and all the work that you do to help our warfighters and the Pentagon be efficient and effective in the IT realm, and for all you do to serve our Nation.

It is one thing that hasn't changed the world of technology since our hearing last year on this topic is the importance of information systems to everything that we do as a nation. IT consumes a massive portion of our defense investment, and cyber continues to be a very high priority for the Department, as well it should be.

However, with this huge investment comes an equal responsibility to make sure that we are conducting proper oversight of those activities. And to that end, I look forward to hearing from the witnesses about the fiscal year 2016 budget request as it relates to our investment in cyberspace, and in securing and modernizing our information systems.

Specifically, Mr. Halvorsen, I would appreciate hearing how the Joint Information Environment [JIE], described as the framework for IT modernization, has evolved and has been implemented. I would also like to hear from each of the services about their understanding and implementation of JIE, i.e., either unilaterally or in conjunction with their sister services, and specific programs associated with this concept.

Conceptually, I support JIE, especially if it provides the ability to better defend the network against outside and insider threats. Yet there is still so much to understand about JIE.

This includes obtaining a solid definition and placing policy guidance associated with implementation, building structures for oversight and management within the Department. And perhaps most relevant today, since it is not an official program of record, building an understanding of how we in Congress can conduct our overseer responsibilities.

As part of this dialogue today, I also expect to hear how the Department will utilize the cloud for both classified and unclassified information, and leverage public, private, and government-owned structures.

Cyber is an extensively, extremely personnel-dominated mission space, and thus is a serious concern when the DOD is confronted with difficulties in recruiting and retaining qualified personnel. I hope the witnesses will take this opportunity to articulate the recruiting and retention challenges in depth, and provide recommendations on how the subcommittee can provide new authorities or other assistance in a National Defense Authorization Act [NDAA] to ensure that we have the best and the brightest cyber IT workforce.

Finally, under the leadership of Chairman Thornberry and Ranking Member Smith, the HASC [House Armed Services Committee] is taking up acquisition reform. Our goal is to take a cumbersome process and make it more agile and flexible, allowing for the finest capabilities to be delivered to our warfighters on time and on budget.

An agile and flexible system is especially important for IT and cyber where technologies and enemy capabilities rapidly evolve and change, and multiple procurement cycles can exist within a single budget cycle. I hope our witnesses will speak to the authorities provided in last year's Defense Authorization Act and elaborate on what more we can do.

With that, again, Mr. Chairman, I want to thank you for organizing this hearing, and to our witnesses for being here today. And I look forward to our discussion.

Mr. WILSON. Thank you, Mr. Langevin.

Before we begin I would like to remind the witnesses that your written statements will be submitted for the record. So we ask that you summarize your comments to 5 minutes or less. And additionally that will apply to the members of the subcommittee.

And as questions are asked we will be limited to 5 minutes based on time of arrival and on either side. And we have a person who is above reproach. Kevin Gates, who will be keeping the time.

And so we will proceed at this time. And we will begin with Mr. Halvorsen and proceed to the right.

STATEMENT OF HON. TERRY HALVORSEN, ACTING DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER

Mr. HALVORSEN. Good afternoon, Mr. Chairman, Ranking Member, and distinguished members of the subcommittee. I am Terry Halvorsen, the acting Department of Defense Chief Information Officer. As such, I am the senior adviser to the Secretary of Defense for all IT matters.

I am responsible for managing the DOD's IT spend so we get more out of each and every dollar, while making sure that the warfighter has the tools to do the mission. My written statement provides you specific numbers and details, but I would like only to highlight some key issues.

One of my key priorities is implementation of the Joint Regional Security Stacks [JRSS]. That is the foundation of the Joint Information Environment. It replaces our current individualized and localized security architecture and systems with a set of servers, tools, and software that will provide better C2 [command and control], more security, and do this at a lower cost. JRSS is an operational and business imperative for the Department.

I want to talk about how we are improving the alignment of our business processes and IT systems and investments. I partner with the Deputy Chief Management Officer, the revised Defense Business Council. We have been directed by the Secretary of Defense to conduct a complete review of all business processes and IT systems in the fourth estate.

That is point one. We will then move into working with my colleagues to do the same review of the military departments.

We are asking the question, what IT business should DOD be directly in, and at what level should we be in it? And I think that is a key question.

We may need your help in changing the business model, particularly in certain areas. We need to look at how we can expand private-public partnership, particularly in the area of data distribution or data centers.

How can I take, in my case, a maybe a DISA [Defense Information Systems Agency] data center, realign it into a more public-private partnership and get full value out of what can be commercial rate improvements? I think we will need to work some legislation to make that easier for all of us to get done.

We are continuing to approve the accounting procedures and have more transparency in our dollars. For example, we have added codes inside the Department that actually show how much money is being spent on data centers and other key IT areas.

We have contract benchmarked within my own organization that has saved $10 million this year, and within DISA $20 [million], and we have seen comparable amounts of savings just by contract benchmarking against industry and other government sectors. I have directed DISA to create an unclassified commercial e-mail solution for the Department.

You have asked about cloud. We put out some new cloud directive. And based on some recommendation from the Defense Business Board, we have changed the way we engage industry and publish our documentation.

We have just published a joint cloud security and implementation guide. And when I mean joint, that was published with the complete cooperation and involvement of industry from the start. We have revised who can buy cloud, allowing the services now to go direct to the provider, not have to go through DISA, and put DISA in a role of being the security standards.

We continue to involve critical areas in mobility with smartphones, wireless and electronic flight bags. I brought two today.

This is the first dual persona unclassified Blackberry. We are now using this. This Android phone is capable of doing up to secret-level security work on it, and it is basically a modified commercial product. And the prices are coming down.

We need to do a comprehensive review of the DOD cyber workforce. But again, I think this an area where we may need help. Somehow we have got to have better movement between government and private industry in the career fields.

We ought to be able to wake up one day, be a private employee and the next day come in and be a government employee and keep that change. I think that expertise, particularly in the area of security we would gain, is vitally important.

In conclusion, we are trying to drive cultural, business, and technical improvements, innovation into DOD's IT to better support our mission and business operations. That requires teamwork.

I am happy to say I have good relations with General Hawkins, the director of DISA; Frank Kendall, who is a strong partner; Admiral Mike Rogers, who I have known for a long time as NSA [National Security Agency] and USCYBERCOM [United States Cyber Command]; Mr. Eric Rosenbach, principal security adviser; and of course my partner in crime, Dave Tillotson, the acting Deputy Chief Management Officer; my colleagues here to the left.

We are expanding our relations with industry, and certainly we enjoy a great relationship with Congress. So I thank you for your interest and support, and I look forward to taking your questions.

[The prepared statement of Mr. Halvorsen can be found in the Appendix on page 27.]

Mr. WILSON. Thank you, Mr. Halvorsen.

General Ferrell.

STATEMENT OF LTG ROBERT S. FERRELL, USA, CHIEF INFORMATION OFFICER/G–6, U.S. ARMY

General FERRELL. Thank you, Chairman Wilson, Ranking Member Langevin, and the other distinguished members of the committee for inviting me to testify today on the Army's network and information technology progress and requirements.

The network and information technology are integral to everything the Army does. Our soldiers and unit training, and mission execution from combat to stability and support to peacekeeping and building, and even the other daily business operations all rely on the network and our information technology systems.

To drive to make the Army more leaner, more agile, and more expeditionary means the network needs to be even more essential. This in turn makes the network and information technology a top modernization priorities for the Army.

We must upgrade our network. In its current state the network remains open to too many threats. However, our future common architecture will enable a secure, joint global network that will provide essential services to our leaders and soldiers, Active, Guard, and Reserve.

Our current network does not have the capacity or capability to do these things. We need sustained funding to upgrade our network.

For the network to do everything that the Army needs, it must have a specific set of characteristics: worldwide reach, guaranteed availability, interoperability with our joint and mission partners, and the ability to accommodate all demands we place on it in a stringent security.

The Army is aggressively implementing capabilities necessary to make this robust network a reality, while also converging multiple disparate networks into a single network.

I recently put in place a comprehensive network campaign plan for the Army. I would like to give you just a brief snapshot of what we are doing to empower soldiers, commanders, and decision makers.

The Army is expanding network capacity and creating an architecture that will allow future growth. Multiple initiatives are under way to strengthen the network security. As a proponent of the Joint Information Environment, the Army has partnered with the Air Force and the Defense Information Systems Agency to implement the Joint Regional Security Stacks, which will reduce the cyber attack surface.

Increasingly effective and efficient network monitoring, management, and defense will address critical operational gaps and mitigate evolving threats. Our initial Joint Regional Security Stack site at Joint Base San Antonio is up and operating.

The Army is also putting considerable effort into development and retention of a highly skilled civilian and military information technology workforce.

Joint cloud computing will have a broad impact on the Army operations. It will enable reliable access to data, application, and services, regardless of the location and the device used. Cloud computing will also allow the Army to introduce innovative capabilities more quickly, and to better focus limited resources on meeting evolving missions' needs.

The initiatives I just mentioned are taking place at the enterprise level, but they all feed directly into enabling the tactical force. The tactical forces we rely on to carry out the National Security Strategy.

Most notably, they provide the foundation for expeditionary mission command, whose success depends on the efficient transition from home station to the deployed theater. Providing soldiers and decision makers a modernized network will require sustained investments, particularly during the modernization cycle that runs through fiscal year 2021.

Additionally, the committee has asked about the impact of sequestration. Sequestration will slow network modernization. In fiscal year 2016 the Army will have to reduce spending on the network services and information assurance by almost $400 million. This cut would impact every aspect of daily Army operations to include training and network security, which could degrade readiness and/or mission execution.

I thank this committee for the opportunity to appear today. The Army and I are grateful for your interest in the network and the information technology needs. I look forward to your questions.

[The prepared statement of General Ferrell can be found in the Appendix on page 36.]

Mr. WILSON. General, thank you very much. And I particularly appreciate your efforts for network modernization. As an Army veteran myself who was trained on SINCGARS [Single Channel Ground and Airborne Radio System], you have come a long way.

General Bender.

STATEMENT OF LT GEN WILLIAM J. BENDER, USAF, CHIEF, INFORMATION DOMINANCE AND CHIEF INFORMATION OFFICER, U.S. AIR FORCE

General BENDER. Good afternoon, Mr. Chairman, Ranking Member, and distinguished members of the subcommittee. I am Lieu-

tenant General Bill Bender, the United States Air Force Chief Information Officer.

In the first 5 months in this position, I have decided to act upon my responsibilities by focusing upon four major lines of effort: enhancing the service's cybersecurity efforts; advancing the Joint Information Environment; developing the IT and cyber workforce by transforming career field development; and finally, operationalizing chief information officer authorities in a way that adds greater value to headquarters Air Force.

My lines of effort are relevant to the myriad of ongoing IT and cyber-related initiatives within the Air Force, and play a critical role in assuring the United States Air Force can accomplish its mission successfully.

First it is important to note cyberspace is an operational domain. It affords us a wider range of operational opportunities, and conversely it exposes us to vulnerabilities and threats that place the Air Force's five core missions, air and space superiority, ISR [intelligence, surveillance, and reconnaissance], rapid global mobility, global strike, and command and control, at risk.

Cybersecurity is at the forefront of my priorities for IT within the Air Force. We must understand and confront the reality that the vulnerabilities we face in cyberspace jeopardize our wartime capabilities, including our aircraft, space, and other weapons systems.

Therefore I have convened under the direction of the Air Force chief of staff a cyber task force with the straightforward objectives of diagnosing the full extent of the cyber threat, developing an enterprise level risk management strategy, informing a better understanding of our priorities for investments.

The momentum toward cybersecurity drives one of my other lines of effort, ensuring the Air Force is a full partner in achieving the Joint Information Environment with the DOD and the other services. We fully understand the imperative to move forward this environment with respect to both operational capability and efficiencies to be gained.

My third line of effort addresses the need to completely transform our IT and cyberspace workforce. It is imperative that we recruit, train, and retain those with the necessary skills to meet IT and cyberspace challenges of the 21st century.

With respect to IT and cyber budgets, the Air Force is partnering with DOD and Air Force acquisition leaders to streamline our acquisition processes. Our Information Technology Governance Executive Board aligns our IT investments and acquisition efforts to the Air Force corporate process.

Additionally remain actively engaged with Air Force Space Command, which is the Air Force's lead major command, with responsibility for the IT and cyber portfolios. Together we are doing what we can to strengthen the investment reviews and requirements management processes.

My office manages the IT Capital Planning and Investment Control process, and leads coordinated and regimented reviews of major investments that are mandated as Exhibit 300s. These reviews will provide greater accuracy on a daily basis, significantly aid the Air Force IT budget and Federal Information Technology

Dashboard reporting process, and enable a process to validate IT requirements and follow our investments.

The lines of effort I have outlined today, if executed well, will deliver the appropriate policies, personnel, capabilities, and resources needed to assure Air Force missions against a determined adversary. I thank you for the opportunity to address the subcommittee, and I also thank you for your interest in these critically important issues. And I look forward to your questions.

[The prepared statement of General Bender can be found in the Appendix on page 53.]

Mr. WILSON. Thank you very much, General.

Dr. Zangardi.

STATEMENT OF DR. JOHN ZANGARDI, ACTING DEPARTMENT OF THE NAVY CHIEF INFORMATION OFFICER, AND DEPUTY ASSISTANT SECRETARY OF THE NAVY FOR COMMAND, CONTROL, COMMUNICATIONS, COMPUTERS, INTELLIGENCE, INFORMATION OPERATIONS AND SPACE

Dr. ZANGARDI. Good afternoon, Chairman Wilson and Ranking Member Langevin and distinguished members. Thank you for the privilege to speak before you today on the Department of Navy's information technology budget. I will keep my comments brief.

There has been an astounding increase in IT capability over the last few decades. It has important implications for the Department of Navy.

However, unlike traditional weapons systems acquisitions, the Department is not driving the pace of innovation. It is industry. The question is how do we leverage what industry is doing now?

Last week I visited forward-deployed naval forces in both Japan and Guam. I met with marines and sailors. I will briefly share with you different perspectives I gained from those interactions.

I met a young aerographer's mate at the Naval Oceanographic Antisubmarine Warfare Command in Yokosuka, Japan. She was in the top three of her A-school class. Most impressively, she advanced from an E1 to E5 in less than 2 years.

She is reliant on the Navy's overseas network to access tactical applications such as the Naval Integrated Tactical Environmental System, or NITES program. Without access to the network and tactical applications such as NITES, she cannot fully support the warfighter mission with meteorological and mission-planning data, despite all her training.

I also met with senior-level leadership in the Western Pacific. Providing mobile, secure command and control, or C2, over forces is an important concern of the fleet, strike group, and unit commanders. Our overseas expeditionary and afloat networks must be able to respond to this demand signal and deliver capability.

The expectations from the Navy and Marine Corps warfighter are high. The reason we need to harness the industry trends of lower cost and more readily available capability is because information technology provides the means to enable better decision making.

For example, if the Department never improves the network or the tactical applications used by the aerographer's mate, she will

not be able to provide the fleet the knowledge products they need to perform their mission or execute it.

Information technology has become the thread that weaves together platforms, tactics, and personnel to execute our strategy. This drives home just how important it is to move forward with transitioning ONE–NET [Outside the Continental United States Navy Enterprise Network] to NMCI [Navy-Marine Corps Intranet], and continuing with installation of Consolidated Afloat Networks and Enterprise Services [CANES] program. Both are absolutely critical in our support of our forward-deployed forces.

Department of Navy programs such as Marine Corps Enterprise Network, Navy Multiband Terminal, Automated Digital Network System, and Mobile User Objective System need your continued support to provide connectivity to the warfighter and afloat and expeditionary warfighter.

In an era of constrained budgets, we need to learn and leverage lessons from industry. It is incumbent on us to reduce redundancy, drive out costs, and deliver innovation.

How we buy more smartly and put technology in the hands of the warfighter? NGEN [Next Generation Enterprise Network]. Our ashore network contract, NGEN, is a true success story that is providing capability now. The NGEN contract delivered $1.2 billion in real savings across the FYDP [Future Years Defense Plan] as a result of competitive market forces.

I believe that we bought smartly. The NGEN contract provides for an enterprise network for both Navy and Marines. NGEN is also how we will deliver JIE and JRSS. We are engaged in the development of JIE and implementation of JRSS.

Data center consolidation and application rationalization are another effort. They are not easy tasks. Industry will tell you that while these are challenging, they are critical components to drive out costs and drive in security.

We are making progress. The desired end state is a single integrated global ashore infrastructure service delivering, leveraging Navy data centers, application hosting, and commercial cloud services. The objective is to drive out cost while still providing the warfighter the information they need when they need it.

Providing increased mobility options to the warfighter is paramount. Putting new industry standard devices that deliver consistent security by separating business data from employee personal information is just starting up, and should be complete by year's end for about 30,000 devices across the Navy.

The Department is focused on innovation. We increasingly realize that information is an asset. The Department's information systems provide an opportunity, and can enable innovation areas of business intelligence and the cloud. We need to rethink how we value and share information. We have to ensure that our processes move at the speed necessary in the information age.

Lastly, Vice Admiral Branch couldn't attend, but wishes to have his statement added to the record. And I would appreciate your consideration there, sir.

The Department of Navy is very proud of our efforts in IT. I am standing by for your questions.

[The prepared statement of Dr. Zangardi can be found in the Appendix on page 62.]

Mr. WILSON. Thank you very much, doctor.

And now we proceed to General Nally.

STATEMENT OF BGEN KEVIN J. NALLY, USMC, DIRECTOR, COMMAND, CONTROL, COMMUNICATIONS, AND COMPUTERS (C4)/CHIEF INFORMATION OFFICER, HEADQUARTERS U.S. MARINE CORPS

General NALLY. Chairman Wilson, Ranking Member Langevin, distinguished members of the committee.

First and foremost I would like to start off my oral statement by stating my number one priority is now and has been for the past 5 years, people, which includes marines and our civilians supporting marines, and are providing support to our forward-deployed forces, which includes marines and sailors. It is my number one priority.

Today, as always, your Marine Corps is committed to remaining the Nation's force in readiness, a force truly capable of responding to a crisis anywhere around the globe at a moment's notice. As we gather here today, 32,000 marines are forward-deployed around the world, promoting peace, protecting our Nation's interests, and securing our defense.

We have marines currently conducting security cooperation activities in 29 countries across the globe and continue to make a difference. All these marines remain trained, well-equipped, and at the highest state of readiness.

Information technology is a key enabler to the Marine Corps being able to fight and win our Nation's battles. As we align our information technology with our Commandants' Planning Guidance and Expeditionary Force 21, we take the approach from the furthest deployed marine and move back to the Pentagon.

This approach, fighting hole to flagpole, allows us to best understand our command and control, and information demands, and to build our networks and programs to support the Marine Corps broad range of missions.

As we look to the future, Expeditionary Force 21 is our corps capstone concept that will increase our enduring presence around the globe. We employ tailored, regionally oriented forces that can rapidly respond to emergencies and crises.

Having the capability to rapidly deploy command and control packages provides a fully joint capable force that can operate as part of a more integrated naval force to better fight and win complex conflicts throughout the littorals.

A key tenet to support Expeditionary Force 21 is the Marine Corps moving towards a single network, the Marine Corps Enterprise Network. The Marine Corps Enterprise Network unification plan provides the Marine Corps path to the Joint Information Environment, or JIE.

We are unifying multiple networks to ensure effective use of our resources, and more importantly to allow reliable access to information for all our forces. Information assurance remains a key component of our Marine Corps Enterprise Network. We have established the Marine Corps Cyber Range to enable the development and test-

ing of information systems, support cyberspace training, and conduct operational planning and realistic exercise support.

Finally, our workforce, the marines and civilian marines who operate and defend the network 24 hours a day, 365 days a year, are our most critical asset. This workforce enables the Commandant's Planning Guidance and Expeditionary 21, and most importantly, supports those deployed marines in accomplishing their mission.

I want to thank the chairman and the committee for the opportunity to appear here today to discuss Marine Corps information technology matters. Thank you for the opportunity to appear before you today. I look forward to answering your questions.

[The prepared statement of General Nally can be found in the Appendix on page 76.]

Mr. WILSON. Thank you, General Nally. And as you cited, 32,000 Marines in 29 countries around the world.

Actually, Congresswoman Stefanik and myself last week saw firsthand at embassies throughout the Middle East and Central Asia the extraordinary young marines providing security. And it would make any and every American very proud. So thank you very much for your service.

General NALLY. Thank you.

Mr. WILSON. As we proceed, and we will be on the 5 minutes for each of us, including myself.

And so first of all, with General Ferrell, because the civilian part of the workforce is so integral when it comes to information technology and cyber, what are we doing to better manage that part of the workforce?

In your testimony you have made some recommendations. Can you please elaborate on some of the things that you would recommend as we should be doing? Do any of the others on the panel have any other and additional recommendations?

General Ferrell.

General FERRELL. Congressman, thank you for that question. The Army is doing an awful lot to increase the capacity, both on our cyber workforce and as well as in our IT workforce.

We have over 11,000 civilian IT workforce that we currently have on the books. And we are implementing a holistic strategy to transform information technology and the cyber workforce, from recruiting to training to training critical parts of the information technology.

From a recruiting side of the house, we have an extensive outreach program that is aligned with STEM [science, technology, engineering, and mathematics] into the high school from K–12, as well as putting on demonstrations to encourage—technical demonstration to encourage the high school students to pursue a career in the STEM world.

We also have the opportunity where we have an internship program where we take high school students as well as college students, about 50 annually a year, and then include them as part of the Presidential Management Fellows. We have about currently three that are on hand working with the Army.

So again, we have the STEM program, outreach with the K–12. And we also have an internship program that we work with the high school students as well as the college students.

On the retaining side of the house, we are also exploring additional incentive pay to promote retention and remain competitive with the industry partner.

And the last piece that—on the training side of the house, the technical programs that we have in place is both from the military side that we offer to advance more technology in the cyber world as well as intel world. And we will offer some civilian opportunities as well. These are some of the programs that we have within the Army.

Mr. WILSON. Thank you very much.

Does anyone else have any to add? Dr. Zangardi.

Dr. ZANGARDI. Yes, sir. Thank you.

Very briefly, on the civilian side from 2012 to 2014 we have seen our attrition rate of civilians drop from 9.7 to 5.1. That may be due to the economy. But I also think it reflects the unique work that we do at locations and SPAWAR [Space and Naval Warfare] Systems Command out in California.

It is a unique opportunity to work on some cutting-edge technology, or also to serve your country. I agree with the general that things like STEM and outreach to schools and other industries to bring in uniquely qualified personnel are very helpful to our ability to keep and retain highly qualified civilians.

On the military side, our rates for accession and retention are being met. We utilize selective retention bonuses and we provide increased training opportunities at the 12- to 14-year mark, which is a mark at which most people will not leave after they get the training.

Mr. WILSON. Thank you very much.

And the next question for me, General Nally, each of you have talked about the personnel challenges related to finding, hiring, and training information technology professionals, both military and civilian. I would like to hear your thoughts on a couple of points. One is leveraging commercial certifications or commercial training.

General NALLY. Thank you, sir. We don't have a problem recruiting and retaining if we are talking to the military first for entry-level Marines. Whether they are enlisted or officers, the training is conducted out at Twentynine Palms, California, at our Marine Corps communications and electronic schools.

The cyber network operators, they actually at the entry-level first formal school, upon graduation they actually receive commercial certifications in four various commercial companies equal to what they would offer for certifications. For example, Microsoft, they depart the school and they have commercial Microsoft certifications.

As they progress in their careers if they decide to stay in they receive additional certifications, i.e., through Cisco, VMware, NetApp are a few of the companies. And all that training is conducted in Twentynine Palms. So we have a formal working relationship with those companies where they actually receive those company certifications.

For civilians I have a budget to train and educate the civilian IT cyber workforce so we ensure that they receive the training, edu-

cation, and certifications that they require for the appropriate billets that they hold.

Mr. WILSON. Well, I would like to congratulate you because I would have thought our retention would be very difficult in the 9.7 to 5.1, doctor. That is incredible because you are dealing with such talented people. Thank you all for your extraordinary efforts to maintain your personnel.

Mr. Langevin.

Mr. LANGEVIN. Thank you, Mr. Chairman. Again I want to thank our witnesses for your testimony today.

Mr. Halvorsen, in 2011 the commander of U.S. Cyber Command briefed the Joint Chiefs of Staff on the inability to see the entire DOD networks, and the risks associated with the limitation. In addition to providing more efficient and effective networks, the Joint Information Enterprise, JIE, initiative is intended to enable U.S. Cyber Command the visibility of the network required to defend it.

In your opinion, is the initiative moving towards that end state? Why or why not? And what official guidance has been provided to the services to ensure that end state?

Mr. HALVORSEN. Sir, thank you.

Yes, we are making good progress on that. The JRSS, as we implemented the first set of software, already exposes more of the network than we had exposed before from CYBERCOM and from the new stood-up DODIN [Department of Defense Information Networks] headquarters which is at DISA, which is now responsible for overseeing that under the operational control of Admiral Rogers.

The services have all been provided guidance, both operational guidance from Mike Rogers, policy guidance from my office, that says we will implement the JRSS. We have laid out the timelines. They are all committed, all team members. You have heard them all testify to that.

We have figured out the funding on how to do this. The next version of the software, which is version 2.0, will complete that picture so that all of the services can see the same picture as CYBERCOM. That is funded.

One of the ways we were able to do that is by looking at some of the business processes in DISA, taking that money and applying it inside of DISA to fund the software. That is step one. And I want to point out that JRSS is the first step.

The next step—and you have heard all of the services talk about how they collapse their enterprise networks. Each of the service entered at a different spot with regard to enterprise networks. They are all working to collapse that.

As we collapse the networks, that will also give us a better picture. It is a little physics. It is less for us to look at. So in addition to putting up the JRSS, we are working with all the services to collapse the total number of networks that frankly Mike has to look at and to make sure that are secure.

Mr. LANGEVIN. And, Mr. Halvorsen, the Joint Chiefs of Staff, Cyber Command, the acquisition community, the services, and many other entities have a stake in JIE. What office, and who, is in charge of this mission?

Mr. HALVORSEN. I own JIE and making sure that that is complete to everybody's satisfaction. Mike Rogers owns it from an operational standpoint. The single point to make sure that it gets done from funding operations is my office.

Mr. LANGEVIN. Okay.

And you described the Joint Regional Security Stack, JRSS, as the foundation of JIE. General Ferrell, you mentioned moving forward with JRSS with the Air Force and DISA, and Dr. Zangardi and General Nally, when will the Navy and Marine Corps move out with JRSS?

And Mr. Halvorsen, what is your view of the different services' timelines? What is each service's programmed investment through the next 5 years in JRSS? And is it equitable and a strategy allowing for the best bang for the buck?

Mr. HALVORSEN. Sir, if you permit me I will first answer that. All of the services are completely committed to this and have funded.

And when we look at what the current condition is, the Department of Navy, and for truth in advertising my previous job was the Department of Navy's Chief Information Officer, collapsed its systems first around NGEN and previous NMCI. They are in some cases better positioned because of that to do and see their network better.

The Air Force and Army are moving very rapidly in that direction. The reason they are moving first behind JRSS is that will give them the same level of capability that the Marine Corps and Navy enjoy now. When the Navy and the Marine Corps, we go to JRSS 2.0, that gives everybody increased capability and everybody will move on that.

The Army and the Air Force will be completed in 2017 migration. The Navy and Marine Corps complete in 2018. That is an aggressive schedule to get all of the networks and the complexity done, but I think it is the right schedule and one that I do not think we can let slip. That is the goal.

You mentioned the "Tank" [Joint Chiefs of Staff conference room]. I briefed the "Tank" two weeks ago. All of the service chiefs are 100 percent behind that and committed to making sure that we do not slip that date.

Mr. LANGEVIN. Anybody else got a comment?

Dr. ZANGARDI. Yes, sir. I concur with Mr. Halvorsen's statement since he had my job previously.

NGEN, the NGEN contract is our path forward to JIE. It—specifically, the technical refresh or modernization dollars within the program will be channeled to JIE activities or acquisitions as the standards are defined.

We are engaged now in engineering, planning, and budgeting on the JIE team. We have engineers involved. We have our SPAWAR folks playing in there. We plan to be part of the definition of JIE and JRSS.

As Mr. Halvorsen said, we will be complete in 2018. We align with that schedule. We are also working closely with PACOM [Pacific Command] J6 on what JIE increment 2.0 is. So we are very involved in the whole effort of JIE and JRSS, and have the mechanisms in place in NGEN to move forward.

General BENDER. Sir, if I could clarify for the Air Force. We are actually at an end-of-life condition. We are on a single security architecture since 2011 with 16 gateways. And this is the next evolution. So JIE, JRSS, is the right way for the Air Force to go.

General FERRELL. And sir, I would like to give you a good news story on the progress of the JRSS, specifically at Joint Base San Antonio where there is a partnership between the Army and the Air Force and Defense Information System Agency.

When we started this journey about a year ago of again taking the JRSS capability, as well as expanding the capacity at Joint Base San Antonio, put it in place and worked through the technical challenges of how do we collapse the network.

I am very pleased to tell you to date that we have expanded the capacity there at Joint Base San Antonio. We have installed the JRSS devices. And we have also passed traffic, both Air Force and Army traffic, over the same network between Joint Base San Antonio as well as Montgomery, Alabama.

So again, that is the first step toward progress, physical progress with this effort. We have taken lessons learned from that initial site and we are going to incorporate that on all the follow-on sites, both CONUS [continental United States] and OCONUS [outside the continental United States].

Mr. LANGEVIN. Thank you.

Mr. WILSON. Thank you, Mr. Langevin.

We now proceed to Congressman Rich Nugent, of Florida.

Mr. NUGENT. Thank you, Mr. Chairman. And I appreciate this panel being here today.

You know one of the things that I always get nervous about when I was over an agency that had computers and every time you have a gateway, a way in, how that opens up. But it is even more troubling as to when you look back at the Snowden incident 2 years ago.

How are we protecting ourselves against an insider attack that could obviously cripple us if that information got out to our adversaries? And I will let anyone take a stab at that one.

Mr. HALVORSEN. Doing a couple things. I mean we have implemented all the directives. And you can see in all of our written testimony, we have complied with all the directives. And we will be implementing a deep insider threat.

But a couple things that I think illustrate what we have done is the biggest insider threat is from systems administrators, the guys that have complete access. We have strengthened the security requirements on those.

We will be in conjunction with Mike Rogers shortly, putting out some more detail on that. It requires them to be token-enabled on our way to making that completely CAC [Common Access Card]-enabled so you will have a visible identity of every system administrator.

We have put in place under Mike's direction, and we could go deeper in a different venue, the ability to see what system administrators are doing and some ability to monitor, I won't say abnormal behavior, but different behavior. When you are in a computer business it is hard.

So if they route traffic differently or if they are seeing some—if we are seeing them move things around differently, that ability is expanding within the Department in addition to all of the things that were directed in the NDAA, which we are on schedule to comply with.

General FERRELL. Congressman, in addition to what my colleague to my right has shared, we are also implementing an extensive educational program to educate our users on identifying the types of malisons that will occur on the network and how to mitigate that.

So again, we are really reaching out to—as well as putting the protection from the software on the computers, as well as monitoring the activities of the administrators, we are also doing the educational aspect as well.

Mr. NUGENT. I know there was a GAO [Government Accountability Office] report out a while back, particularly as it relates to DISA, but as it relates to JIE that it is so broad that there is no one program administrator. Were they correct in that assumption? Or was——

Mr. HALVORSEN. I think there was certainly some truth that we were a little fractured in what we had defined JIE. So with the help of my colleagues over the last year what we did was take a look at what is JIE.

JIE is a concept. We are not going to ever implement JIE. What we will implement is the steps that get us to a Joint Information Environment.

So what I can now tell you, and I think you have heard today, the first step of that is to get to the Joint Regional Security Stacks, phase one. Phase two is for us to then—how do we implement and take that into our mission and coalition partners. So they are the first two key, very physical, very visible, measurable.

You can put metrics on them, steps that we have to do with JIE. And I think we had not clarified that really, simply, until the last year. And that is—that may be what was the single biggest driver is that we really did clarify. Those are the key points that have to happen in that sequence.

Mr. NUGENT. All right. It makes sense because obviously if you have one agency or one group that is in charge of all of the IT for all the services there are some real gaps that would occur. Things the Air Force would be important to would not be as important to the Army or vice versa.

So I think that your concept is great. And I think that you have—through the services you have some great folks that are very talented that can move this forward.

You know IT is always something changing. I can remember my past life it always seemed like you know we just upgraded our servers and then it wasn't 2 years later saying hey, boss, the stuff is no good. We got to get new stuff.

And I am sure you face that same type of environment. But how do you guard against that, I mean constant change over what you need, equipment? And I don't know if you can.

Mr. HALVORSEN. I think you have to do two things. I mean one of the things that this group has done is decide about some ways that we will all look at certain investments.

So we now have within this group a standardized business case analysis process. And when I say business case, our business is war.

So it also looks at the operational pieces, too. It is not just on the business systems. That is one way that we can all look and make sure that we are looking at things and measuring the same way.

It is okay for things to be different, particularly in the physical properties, different equipment, as long as it will perform to the same standards. It measures up to the same money, accountability, and all the other measures. We are doing better at that.

We are also looking at what is our current inventory of not just things but software and applications. One of the things that we are looking at now is how do our applications line up? I will give you an example.

When we look at logistics, about 80 percent of our logistics applications share a large majority of data elements that are the same. And I think that is the other change.

You really have to go to the data level. If those data elements are the same, maybe the first thing that we can do is start shrinking the number of systems, let the applications that the services need, because they do need to be distinct in some areas.

You pointed out right the Air Force, the Army, the Marine Corps they have different requirements on some of this. We can combine the data elements and wrap that. That is not a great term.

Wrap that around the different parts of the applications that each of the services need, share common data, protect it in one location. And it both reduces costs and improves your operational capability. We are looking hard at how we expand that effort.

Mr. NUGENT. I appreciate that.

And, Chairman, thank you for indulging me——

Mr. WILSON. Here, here.

Mr. NUGENT. Thank you.

Mr. WILSON. Thank you very much, Sheriff Nugent.

We now proceed to Congressman Jim Cooper, of Tennessee.

Mr. COOPER. Thank you.

I am worried we are already in a cyber war, we are just not admitting it. I don't remember from history a time in history of warfare when more eggs have been put in one basket, basically.

Virtually every chip in the world being made in one country that is not here. And the software is so unimaginably complex it is almost impossible for human beings to figure it out. So I am worried that the acronym "CLOUD" really stands for the "Chinese Love Our Uploaded Data."

I worry that none of the witnesses that I have ever heard calls for a change in the UCMJ, the Uniform Code of Military Justice, so that computer security becomes a value to be preserved because computer hygiene is staggeringly important. And perhaps there has been testimony to that effect. I haven't heard it.

I am worried that our troops would be incapable of working if the Net went down and things go dark. I don't know anybody knows the degree of Internet of Things when facilities could be shut down, as relatively unprotected.

And I don't know. Maybe you have been red-teaming all this. But to me the vulnerability is amazing when virtually every major U.S. company has already been taken down to some extent. Entire countries like Estonia were almost put out of commission years ago by hackers.

I just worry there is more vulnerability here than perhaps this hearing has indicated so far.

Mr. HALVORSEN. Sir, I don't think we could tell you that we are perfectly secure. I think that would be a bit ridiculous statement to make. What I can tell you is that we are doing the things you talked about.

And you talked about accountability. And I will get you a copy of the recent memo. But we did working together have the Deputy Secretary of Defense for the sign out a recent memo that improved accountability in how we hold individuals, both civilian and military, more accountable for their cyber actions. That is working.

We have had recent discussions about how do we raise the bar on cyber hygiene. As we have had our discussion with the cloud, I will tell you that the most contentious issue with industry—we are not dodging the hard question of how they will meet our requirements, and then frankly how will they respond when they have a penetration and lose our data?

What is the accountability that they are going to have. It is one of the things right now that is slowing the higher level cloud movement because we have not worked that out.

Industry has not yet said that they will abide by some of those rules. We are certainly open to them showing us different technology to do that. But they still have to show us that they are doing it. So we are having that dialogue.

We are looking at what it means to be cloud. So maybe I should expand just a minute on that. We are not going to just use commercial cloud. We will use every hybrid there.

DISA has the milCloud. And to their credit, they have dropped the rates so it is more competitive with commercial. But what it does do is it provides that extra level of security for the really valuable data that we just can't afford to lose.

The commercial world is working to move up to those standards. And as they do, we will put more into the cloud, but not until they meet those requirements. We are not lessening our security requirements. In some cases we are standardizing them. In other cases we are raising them.

And the conversation with industry, which they did not like but were happy to be engaged in, the way we are publishing the cloud documents, what we have had to tell them is the standards I put out today in this environment, in the IT world, they will change. And they might change in 6 months, depending on what the threat does. And we have told them they have to be reactive to that.

We are not going to put anything out there that does not meet the standards and that we have not looked at. And we are increasing the amount of red-teaming that we are doing across the board.

Mr. COOPER. So we don't need to change the UCMJ?

Mr. HALVORSEN. I don't think we need to change the UCMJ today. I will tell you I think we need to enforce some of that. And

it is not just the UCMJ because that would only govern our military as you know, but also the civilians.

We have got to enforce the policies. And I think that is mostly about educating the commanders on how they do that. The policy is there.

Cyber presents some problems even from the forensics side of how do you know who put it in. One of the reasons that we are doing more PKI [public key infrastructure]-enabling and getting down to the single identity is that when you put it in we will know.

Once we have that I think you will see. And we are getting that more and more across the board. We have it on some systems. You will see us be able to actually hold an individual accountable for making a bad action on the network.

Mr. COOPER. Thank you, Mr. Chairman.

General NALLY. I think—sir, if—just a minute. This might make you feel a little bit better, but three quick things. One, the Marine Corps is going toward using a private cloud.

Number two is in terms of what you mentioned about the UCMJ. We have actually published a document states we call it a negligent discharge. If a marine or civilian takes classified information and does something inappropriate with it, whether puts it on a NIPRNET [Non-Secure Internet Protocol Router Network] or we had a spillage, et cetera.

We do hold them accountable, the commanders do. So we let the commander, whoever the commander is, know that this individual had a negligent discharge. They hold them accountable.

And three is we actually are training for a SATCOM [satellite communications] degraded intermittent latent environment, stressing VHF [very high frequency], UHF [ultra high frequency], HF [high frequency], terrestrial types of equipment, commander's intent and mission type orders. So we are pushing that down to the lowest levels.

Dr. ZANGARDI. Sir, may I respond?

A couple areas. First, modernization is capability and security. Our NGEN program has built in modernization so we bring in technology on a 4- to 5-year refresh basis.

Our afloat network CANES has a 2-year software upgrade and a 4-year hardware upgrade built in. So as you do modernization you bring in the latest technology, bring in the latest security.

Operation Rolling Tide, ORT, dollars are in the budget. That is bringing out tools, techniques, procedures to our folks out in the fleet that will improve security on our afloat and ashore units.

We stood up in the Navy something called TFCA, Task Force Cyber Awakening. And I will read exactly what it does. It delivers fundamental change to the Navy's organization, resourcing, acquisition, and readiness. And align and strengthen authority, accountability, and rigor in Navy cybersecurity.

We have full, broad support across the Navy organization. My boss, the Assistant Secretary for Research, Development and Acquisition, is the lead for the EXCOM [Executive Committee], along with the Vice Chief of Naval Operations. The three-star SYSCOMs [System Commands] are involved, all the resource sponsors. It has the highest level of interest.

With regards to the cloud, I align with the DOD CIO on that. Before we move any data out to the public cloud, we are going to go through the data and screen it very carefully to make sure that we are not putting things, data, in commercial cloud scenarios that we should not be putting it. We are going to proceed with due caution.

And to add on to General Nally, working, deploying in a degraded environment is key to Navy in the Western Pacific. We need to have the procedures in place to do that. And we are working those.

Mr. COOPER. Thank you, sir.

Mr. WILSON. Thank you, Congressman Cooper.

We will now proceed to Congresswoman Elise Stefanik of New York.

Ms. STEFANIK. Thank you, Mr. Chairman. And thank you to all of our witnesses for your testimony today.

General Ferrell touched on this briefly, but I wanted to ask each of you to weigh in. In your view, what are the risks and vulnerabilities to our network campaign plans, network modernization efforts, should DOD be forced to execute funding levels at BCA funding levels?

Mr. HALVORSEN. In the short term we will lose 2 to 3 years. And that really sums it up. We will fall 2 to 3 years behind. You have heard the specific numbers. There are specific numbers in testimony. Sequestration will delay the modernization 2 to 3 years.

And that comes with all of the things you have heard today. If we don't do that we will be more vulnerable. We will maybe, using your definition, sir, of "CLOUD" if we don't get some modernization. We won't support the warfighters. They will be at risk.

Ms. STEFANIK. And could you add on also what that means for the current threat assessment, how the threats have increased over the past 5 to 10 years?

Mr. HALVORSEN. I can tell you that they have increased in this form over the last 3 to 5 years. They are certainly more capable. And that includes everything from your country state threats to terrorist groups that would be in the news today.

Any slowdown in our modernization will make it easier for even less complicated or less sophisticated groups to interfere with our business. It will expand the number of threats we will have to face if we don't carry through with some of the modernization and some of the security changes we are making. And they will be delayed by sequestration.

Ms. STEFANIK. Would anyone else like to add?

General BENDER. I will add just very briefly that I am relatively new in the position. But 5 months of discovery leaves me with a very strong impression that we are not going to harden or protect our networks to a completely safe, secure environment. It is nearly impossible because of the evolving nature of the threat.

That said we need to have, and as the other services have already mentioned, the ability to fight through a determined adversary and find our way through it. And so risk management becomes really what is key and essential to our approach going forward.

Dr. ZANGARDI. As I mentioned in a previous question, modernization is fundamental to providing us security and the capability we

need. Sequestration will hamper, slow by several years our ability to modernize our IT capability.

General NALLY. Our biggest concern is people. So if we have to reduce funding and then the people that actually defend and protect the network, and we have to let those people go. That is our concern.

And again, that gets back to my first priority. It is the people. If I don't have the right people to operate and defend the network, the network is worthless.

Ms. STEFANIK. Thank you. I have one question on a separate topic. And this is for just my background and for everyone else on the committee.

Can you give an assessment of where other countries are in terms of their investment in network modernization efforts? Are we behind? Are we losing our edge? I know that is a very broad question, but it is an important one.

Mr. HALVORSEN. I don't think we are losing the total edge. Do I think that particularly if we get sequestration, which would not impact, say some larger countries in the world that we were all concerned with? They will gain.

I mean that is a fact. I think right now we are in a good position in terms of the edge. But in IT that edge can disappear so very quickly.

And very candidly, this is public knowledge that the Chinese, the Russians, other groups are making investments in all of these areas. If we are not able to continue our plan we will lose some of that edge and they will gain capability.

Ms. STEFANIK. Thank you very much, unless anyone has anything else to add. Thank you. I yield back.

Mr. WILSON. And thank you very much for your terrific questions. We appreciate that, and Mr. Langevin.

At this time I would like to again thank each of our witnesses for being here today.

I want to thank the subcommittee members for their participation. And then, of course, Kevin Gates has just been extraordinary sitting here quietly maintaining time.

And for each of you, thank you for your service. It is so important for our country.

We are now adjourned.

[Whereupon, at 5:12 p.m., the subcommittee was adjourned.]

A P P E N D I X

FEBRUARY 25, 2015

PREPARED STATEMENTS SUBMITTED FOR THE RECORD

FEBRUARY 25, 2015

STATEMENT BY

TERRY HALVORSEN

ACTING DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER

BEFORE THE

HOUSE ARMED SERVICES COMMITTEE

SUBCOMMITTEE ON

EMERGING THREATS & CAPABILITIES

ON

"Information Technology Investments and Programs: Supporting Current Operations and Planning for the Future Threat Environment"

FEBRUARY 25, 2015

NOT FOR PUBLICATION UNTIL RELEASED BY THE SUBCOMMITTEE ON EMERGING THREATS & CAPABILITIES, HOUSE ARMED SERVICES COMMITTEE

Introduction

Good afternoon Mr. Chairman, Ranking Member, and distinguished Members of the Subcommittee. Thank you for this opportunity to testify before the Subcommittee today on the Department's information technology (IT) budget request. I am Terry Halvorsen, the Acting Department of Defense (DoD) Chief Information Officer (CIO). Since May 2014, I have served as the principal advisor to the Secretary of Defense for information management, IT, cybersecurity, satellite communications, positioning, navigation and timing, spectrum, and nuclear command, control and communications matters. My office provides strategy, leadership, and guidance to create a unified information management and technology vision for the Department and to ensure the delivery of information technology based capabilities required to support the broad set of Department missions.

As the DoD CIO, I have one imperative – to ensure that warfighters have the right IT/Cyber, secure communications equipment and capabilities they need to execute the missions given to the greatest fighting force in the world. In my capacity as the senior civilian advisor to the Secretary of Defense for IT, with responsibility for all matters relating to the DoD information enterprise, my office is driving cultural, business and technical innovation at DoD by better integrating our IT infrastructure, improving alignment, business process improvement, and supporting agile and innovative IT acquisition. This will help change how people at DoD are able to use IT, enabling support to their missions in new, improved ways, whatever the mission requires, from the desk to the desert. Although our prime business is warfighting, DoD is an expansive organization with responsibilities that go beyond warfighting, and include the areas of logistics/supply, personnel, finance, and medicine, among others. If DoD were a Fortune 100 company, it would be at the top of the list. We must adopt the cost culture and practices of the top performing companies to insure every dollar is accounted for and that to the greatest extent possible, we spend those dollars on the business of warfighting.

Today I would like to provide you with an overview of the Department's IT budget, the importance of IT and cybersecurity to our warfighting and business missions, and what we are doing to better manage DoD's IT spend to get more out of each and every dollar. I will highlight the Department's progress in implementing the Joint Information Environment (JIE) – specifically the Joint Regional Security Stacks (JRSS), efforts to strengthen the IT investment review and requirements management process, how we are improving relations with industry, as well as strengthening the IT workforce.

Overview of DoD's Information Technology

The Department's Fiscal Year (FY) 16 IT budget request is $36.9 billion. This request includes funding for a broad variety of IT, ranging from DoD warfighting, command, control, and communications systems, computing services, cybersecurity, enterprise services like collaboration and electronic mail, and, intelligence and business systems. These investments support mission critical operations that must be delivered both on the battlefield and in an office environment. They also provide capabilities that enable the Commander-in-Chief to communicate with and direct the military, and that support command and control, intelligence, logistics, medical and other warfighting and business support functions throughout the Department. The overall IT budget includes a request for $5.5 billion for the Department's cyberspace operations and activities. These are designed

to ensure that essential Department missions work well in the face of growing cyberattacks. These cyber efforts continue to receive the highest-level attention and support of the Department.

DoD CIO Priorities

Joint Regional Security Stacks (JRSS)

One of my immediate priorities is to implement the Joint Regional Security Stacks, which are the first or foundational phase of the JIE. JRSS are a regionally based, centrally managed rack of servers, switches, and other equipment that will replace the current set of separate, individualized, localized Service and Agency security systems. This will help to ensure that the Department's facilities are using the same security architecture in order to move toward JIE. This approach takes into account that Military Department, Agency, and Combatant Command cyber and IT environments differ, which results in differing mission-based priorities. They will enable the operations commander and service partners to see a common network picture.

As of today, JRSS version 1.0 has been installed at 10 sites with traffic migration underway at the Defense Information Systems Agency (DISA)'s Defense Enterprise Computing Center (DECC) Joint Base San Antonio (Ft Sam Houston for Army and Lackland/Kelly Air Force Base for Air Force) and failover location DECC Montgomery. The JRSS version 1.0 capabilities enable the Army to sunset their local security enclave protections. Additionally, Joint Management System version 1.0 has been installed at DECC Joint Base San Antonio. This critical phase of the JIE began with the purchase of 15 JRSS for DoD's non-secure Internet Protocol Router Network (NIPRNET) and network upgrade components, which included bandwidth upgrades and Multi-Protocol Label Switching (MPLS) routers, by the Army through DISA in late FY13. The JRSS effort expanded in FY14 and this current fiscal year (FY15) to include Army, Air Force and DISA, the Navy, Marine Corps and Defense Health Agency (DHA) will begin migration work behind the JRSS in FY17.

The FY16 budget request for the Services, DISA, and DHA includes funding to purchase and implement JRSS version 1.5, network upgrade components, and JMS version 1.5 improvements. These investments will provide a global implementation of JRSS 1.5 for NIPRNET; the associated Department of Defense Information Network (DODIN) enhancements will result in for greater bandwidth and enhanced traffic routing and security, and enable the Air Force to sunset their Air Force Network Gateways in FY16.

In FY17, the JRSS version 2.0 will provide capabilities for the Navy, Marine Corps and DHA that will allow these components to sunset their individual gateways and fully leverage the JRSS and network upgrades. DoD is also in the process of planning the installation of 25 JRSS across the globe for the Secret Internet Protocol Router Network (SIPRNET).

When completed the JRSS will provide a more secure environment with improved command and control that operates at lower cost.

Mission Partner Environment/Network (MPE/N)
We are working to develop a more commercially based and robust mission partner environment/network. This approach will provide a more cost-effective, rapidly reconfigurable and multi-level data protection network. It will provide full data media capability to support operations in all environments, with the ability to rapidly add and subtract mission partners. This is a top requirement for all Combatant Commands.

Business Process Systems Review (BPSR) – Improving Alignment of Business Processes and IT Systems
The BPSR is a partnership between my office and that of the Deputy Chief Management Office (DCMO), currently led in an acting capacity by Mr. David Tillotson. Together we are co-leading the Defense Business Council, a review of business processes and the supporting IT systems within the Fourth Estate. We are working with the Defense Business Board (DBB) and industry experts to examine how we do business in the Pentagon and how we can do better. We are exploring the potential to increase government/industry partnerships in diverse areas such as data distribution, with the goal of creating a less costly platform while maintaining our stringent security standards. We are asking the question what businesses do we DOD need to be in and to what level. For the CIO office specifically this means asking what IT businesses should DISA be in and to what level. Based on this question and looking at the available data, I have directed DISA to make the next offering of DISA Unclassafied E-mail a purely commercial solution. I believe this will result in a 20-25% reduction in email costs. The BPSR review will provide the Secretary's senior civilian advisors with information to help them clarify whether their organizations are aimed at Department-wide outcomes and to identify any resources allocated to these outcomes. This effort also identifies potential obstacles to achieving the outcomes such as resource shortfalls and process obstacles, as well as activities that might be improved or eliminated. The overall goal is to increase mission effectiveness, through increased alignment of processes and systems; better understanding of the interrelationships between processes and systems; and to lower the overall costs of doing business through the implementation of cost-driven metrics. Within the office of the CIO, by reviewing contract benchmarks we were able to reduce spend by $10M this year. We were also able to reprogram $20M from DISA contracts without reducing contract work to support JRSS installs. DISA also lowered its rates by 10% and is on track to do the same next year. ,. These are just first examples and by the summer we will have more examples totaling substantially more dollars. The Defense Business Board is providing leaders from key industry sectors like IT and working with us to find area where we can quickly adopt new ideas and practices. One of which is how we are changing the approach to cloud computing.

Cloud Computing
Cloud computing plays a critical role in the Department's IT modernization efforts. Our key objective is to deliver a cost efficient, secure enough enterprise environment (the security driven by the data) that can readily adapt to the Department's mission needs. The cloud will support the Department's JIE with a robust IT capability built on an integrated set of cloud services provided by both commercial providers and DoD Components. We will use a hybrid approach to cloud that takes advantage of all types of cloud solutions to

get the best combination of mission effectiveness and efficiency. This means in some cases we will use a purely commercial solution, which we have done with Amazon on public facing data, in others we will use a modified private cloud hosted in commercial solutions, an example could be a shared federal or federal state government cloud, and for our most protected data a DOD private cloud that uses best industry practices.

In the past year, the Department has made significant progress in adoption of cloud. My office completed a major revision to security requirements for commercial and DoD cloud service providers. The resulting Cloud Security Requirements Guide (CSRG) was published on January 12, 2015. In January, we also hosted a DoD cloud day open to commercial cloud service providers, media, and Federal government partners to underscore our message for DoD's new approach to cloud and promote an open dialog between the Department and industry. We are publishing our guides in collaboration with industry and producing truly interactive agility from the commercial and government sector. We have received very positive feedback from industry on this approach.

My office has issued revised guidance on the acquisition and use of commercial cloud computing services, that describes how DoD Components may acquire commercial cloud services and how they are responsible for determining what data and missions are hosted by external cloud service. We have opened the acquisition aperture and services may acquire cloud service directly, using the published guidelines.

In addition, DISA achieved initial operating capability (IOC) for its Cloud Access Point (CAP) in November 2014. The CAP provides an open and standardized means to integrate the computer network defenses between the DODIN and Cloud Service Providers (CSP) thus protecting all DoD missions from incidents that may adversely impact a CSP. DISA also achieved IOC for milCloud, the intended private cloud infrastructure for the DoD, in January 2014. The DISA MILCLOUD is much closer to commercial rates and provides additional security protection. As we continue to move forward in this area, we are improving mission effectiveness, increasing security and realizing efficiencies.

Mobility

DoD continues to evolve areas critical to mobility: the networking infrastructure, devices, and applications. The goal is to reduce the cost of accessing information while integrating a security strategy that protects the data and incorporates the most recent commercial technologies. Specific examples of DoD mobility initiatives include: an effort to simplify the ability to encrypt and authenticate email, layering multiple commercial standards permitting smart phones/devices manufactured by vendors such as BlackBerry, Samsung and Boeing, to handle secret data and the use of commercial cloud providers to globally distribute and synchronize flight information for the Air Force's Electronic Flight Bag program. We are also expanding the use of wireless capabilities.

Key partners in these efforts are DISA and the National Security Agency (NSA), who working together with industry, have developed security protection profiles for several of the major smart phone technologies. The Services are also actively involved in these efforts and are develop mobility applications for a broad range of DOD missions including recruitment, training, logistics (Inventory Management), maintenance, navigation and command and control.

IT/Cyber Workforce
DoD is implementing a comprehensive strategy to transform multiple segmented, legacy personnel management constructs into a cohesive, mission-focused DoD Cyberspace Workforce Framework (DCWF). This effort will enhance the Department's ability to recruit, train, develop, and deploy a workforce capable of interoperating across organizational structures to provide IT, cybersecurity, intelligence and operational capabilities. The DCWF will be the cornerstone of the DoD effort to standardize cyberspace workforce identification, tracking, qualification, and readiness.

To date, DoD has completed coding of over 30,000 DoD IT Management positions (OPM series 2210) with new cyberspace workforce nomenclature. This effort is in the pilot phase to align DoD personnel under the DCWF, while also meeting OPM workforce coding mandates and intent of the National Initiative for Cybersecurity Education (NICE) Workforce Framework. We are also developing new cybersecurity curriculum for the Defense Acquisition University to enhance secure acquisition of information systems and IT, and mitigate supply chain risk. Finally, we are pursuing Joint Professional Military Education accreditation for cybersecurity leadership master's degree at the National Defense University iCollege.

IT Personnel Exchanges with Industry
Section 1110 of the FY10 National Defense Authorization Act (Public Law 111-84) authorized DoD to establish a Pilot Program for the Temporary Exchange of IT Personnel, referred to as the ITEP pilot. While there has been limited participation to date, the assignments thus far have been mutually beneficial to DoD and private industry, and DoD has found the authority provides a valuable tool for exchanging innovative ideas with industry. ITEP allows DoD and industry to each experience the challenges each other faces in managing their IT acquisitions, infrastructure and security requirements, and to exchange best practices on these issues. ITEP allows both DoD and private sector IT employees who work in the IT field (including areas such as system administration, IT project management, network services, software application, cybersecurity, enterprise architecture, internet/web services, data management and system analysis) to participate in a temporary detail to the other sector in order to gain a better understanding of each other's' technology practices and challenges. ITEP is not a 1-for-1 exchange of personnel. Instead, it is an opportunity for the exchange of knowledge, experience, and skills between the DoD and private sectors. Private sector includes nonpublic or commercial individuals and businesses, nonprofit organizations, academia, scholastic institutions, and nongovernmental organizations.

Since 2007, there have been three industry participants that have gone through the program for six – twelve month assignments. These exchanges were positive experiences and highly beneficial to all parties. A Cisco employee is currently detailed under this program to my office, and is assisting with planning, transition, and consolidation of DoD IT systems and services. My office has established relationships with industry and non-profit organizations to increase the overall utilization of this program.
We are also for the first time going to send civilian employees to industry to gain experience in technology and business practices.

Management of Defense Information Technology Systems
The Department is aware of recent Congressional actions and intentions to expand oversight and architecture requirements for DoD IT systems. However, under the recently restructured Defense Business Council, which I co-lead with the Acting DCMO, the Department is actively changing its internal processes to improve that oversight. We believe that the authority already contained within the Clinger-Cohen Act, as well as 10 U.S.C. 2222, is sufficient to allow the Department to more carefully and thoroughly oversee its IT systems and processes. The Clinger-Cohen Act gives the authority and responsibility for information technology enterprise architecture development and management to the CIO. DoD CIO manages its architectural processes using the mission area construct with active involvement of the mission area leads and Principal Staff Assistants. I would also urge the retention of the existing anti-deficiency act language in section 2222 related to obligation of funds. This language is essential for the investment review board's enforcement of the review process and associated decisions. While improving and realigning oversight of information technology systems, the Department looks forward to working closely with the Congress to ensure we are meeting Congressional intent.

Supporting Agile and Innovative IT Acquisitions
The Department's Better Buying Power (BBP) Initiative, as launched by Undersecretary Kendall, is based on the principle that continuous improvement is the best approach to improving the performance of the defense acquisition enterprise. This effort follows the evolution of the two prior BBP efforts with a shift in emphasis toward achieving dominant capabilities through innovation and technical excellence. For the DoD CIO, BBP 3.0 follows onto some things that we are already doing, such as expanding the number of enterprise buys, continuing efforts on enterprise licensing, and working to expand into enterprise hardware. We do understand that we don't drive the business IT market place, Industry does. We can if we are smarter buyers and engage better with industry to understand how the cost dynamics influence the market space and achieve improvements in effectiveness and efficiency. This new focus is important to driving cultural innovation at DoD. In simple business terms, generally buying more of a commodity will lead to a better pricing (much of business IT has been commoditized) and purchasing off an existing contract is quicker than starting a new contract.

Conclusion
In closing, at the DoD CIO we are driving cultural, business and technical improvements and innovation into DoD's IT to better support our mission and business operations. To implement the activities described above and achieve the innovations and transformations necessary in the future requires the efforts of my office, the Department's leadership, and Congress. Lt. Gen Ronnie Hawkins, the Director of DISA, is a key partner in each of these efforts. My office also enjoys a strong partnership with the Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, under the strong leadership of Mr. Frank Kendall. Similarly, I have a close relation with Admiral Mike Rogers, in his capacity as both Director of NSA and Commander of U.S. Cyber Command. I continue to work closely with the recently established Principal Cyber Advisor, Mr. Eric Rosenbach.

Finally, as I mentioned above, I partner with Mr. David Tillotson, the Acting Deputy Chief Management Officer, on all DoD business management issues.

My goal is to change how we in DoD are able to use IT, enabling support to their missions in new, improved ways, whatever the mission requires, from the desk to the desert. We are working to do this more effectively and efficiently and to not ever forget that our prime business is supporting the warfighter. I want to thank you for your interest and continued support in Department's IT initiatives and look forward to your questions.

Terry Halvorsen

Acting Chief Information Officer

Terry Halvorsen was selected to serve as the Acting Department of Defense Chief Information Officer effective May 21, 2014. He previously served as the Department of the Navy Chief Information Officer.

As the Acting DoD CIO, Mr. Halvorsen is the principal advisor to the Secretary of Defense for Information Management / Information Technology and Information Assurance as well as non-intelligence space systems, critical satellite communications, navigation, and timing programs, spectrum and telecommunications. He provides strategy, leadership, and guidance to create a unified information management and technology vision for the Department and to ensure the delivery of information technology-based capabilities required to support the broad set of Department missions.

Before serving as the Department of the Navy CIO, Mr. Halvorsen was the deputy commander, Navy Cyber Forces. He began serving in that position in January 2010 as part of the Navy Cyber reorganization. Previous to that, Mr. Halvorsen served as the Deputy Commander, Naval Network Warfare Command. He was responsible for providing leadership for over 16,000 military and civilian personnel and supporting over 300 ships and approximately 800,000 globally dispersed computer network users. In this position he was responsible for the business performance of Navy network operations, space operations, information operations and knowledge management.

Mr. Halvorsen retired from the Army after serving as an intelligence officer in a variety of assignments, including Operations Just Cause and Desert Storm. He holds a bachelor's degree in history from Widener University, and a master's degree in educational technology from the University of West Florida. He is a Rotary International Paul Harris Fellow and an Excellence in Government Leadership Fellow.

RECORD VERSION

STATEMENT BY

LIEUTENANT GENERAL ROBERT S. FERRELL
CHIEF INFORMATION OFFICER/G-6,
UNITED STATES ARMY

BEFORE THE

HOUSE ARMED SERVICES COMMITTEE
SUBCOMMITTEE ON INTELLIGENCE, EMERGING THREATS
AND CAPABILITIES

FIRST SESSION, 114TH CONGRESS

INFORMATION TECHNOLOGY INVESTMENTS AND PROGRAMS: SUPPORTING CURRENT OPERATIONS AND PLANNING FOR THE FUTURE

FEBRUARY 25, 2015

STATEMENT BY
LIEUTENANT GENERAL ROBERT S. FERRELL
CHIEF INFORMATION OFFICER/G-6, UNITED STATES ARMY

Chairman Wilson, Ranking Member Langevin and other distinguished members of the committee –

Thank you for inviting me to speak to you today about the Army network and information technology. Much has changed since an Army CIO last testified in 2009 and I appreciate the opportunity to give the subcommittee an update.

Information technology and the network are at the heart of everything the Army does. Whether it's day-to-day business operations, such as paying service men and women, taking care of Families and running our installations; or training our Soldiers so that they are fully prepared and ready for anything we may ask of them; or executing the missions assigned by the president and our combatant commanders, to include combat, humanitarian, stability and support, and partner-building operations, the Army relies on the network and our IT systems to get it done. As we draw down end strength, we expect the role of the network to grow, particularly from an operational perspective. To remain effective on the battlefield and reduce the requirement for forward-deployed Soldiers, the Army will need more rigorous and realistic training, even better situational awareness and understanding, more effective mission command, a smaller logistical footprint and greater lethality. The network is key to achieving all of those objectives.

With that in mind, the Chief Information Officer/G-6 team this month completed and published the Army Network Campaign Plan. This plan, along with the accompanying implementation guidance for the near and mid terms, sets the path to providing the Army the network capability it will need to remain the world's preeminent land force. It was designed to support all aspects of the Army's new operating concept: provide a foundation for joint operations; deploy and transition rapidly; develop the situation in close contact; maneuver from multiple locations and domains; operate while dispersed yet maintain mutual support; integrate with our action partners; and present multiple dilemmas to the enemy. With sustained investment, we believe the Army will achieve the envisioned secure, integrated, global network by the end of fiscal year 2021.

It's important to first lay out the overall environment we expect to face. Taking our current global posture as a benchmark, we believe the Army will remain in high demand. As the chief of staff, Gen. Odierno, testified in January, the Army is fully engaged, with nearly 140,000 Soldiers and nine of our 10 division headquarters committed, deployed or forward-stationed in nearly 140 countries on six continents. Given the tumult in the Mideast, Southwest Asia, Africa and Europe, it is unlikely this operational tempo will decrease in the near future. Our adversaries are becoming more sophisticated and their access to cutting-edge technology, especially information technology, is getting easier. At the same time, that technology is evolving at a rate that outpaces our acquisition processes, making it difficult to keep our Soldiers equipped with the best available systems and capabilities. Additionally, the threat to DoD networks continues to intensify; the department is the target of millions of cyber intrusion attempts every day. As I'm sure you are aware, the

consequences of a successful attack could be quite severe. The backdrop to these conditions is a national fiscal picture that indicates lower budgets for the Army and DoD.

For the Army to achieve success in this environment and fulfill the training, operational and business requirements I described earlier, the network must have a very specific set of characteristics: worldwide reach, whether at home station, en route, upon early entry or in a mature theater of operations; guaranteed availability, regardless of the number of users or the location, to include the most austere operational conditions; and a level of security that protects the integrity of the network itself and the data it carries. The bottom line objective is to provide all authorized personnel access to the information, services and capabilities they need, anytime, anywhere.

To achieve this network, the Army Network Campaign Plan establishes five lines of effort (LOEs), or priorities. The first is to provide Signal capabilities to the entire force. This LOE will synchronize delivery of network capacity, security, services, training and doctrine. LOE 1 also will develop a Signal equipping strategy to deliver intuitive, secure, standards-based capabilities that are adaptive to the commander's requirements and integrated into the Common Operating Environment.

LOE 2 focuses on enhancing cybersecurity capabilities by optimizing defensive cyberspace operations and DoD Information Network operations. This LOE will improve the network defense posture by minimizing the attack surface, establishing physical path diversity at critical installations, strengthening data defenses and enhancing security

through cyber hygiene and best practices. The Army intends to transform cyberspace defensive operations by deploying capabilities that support cyberspace defense. We also will enhance cyberspace situational awareness by improving the cyber-sensing infrastructure, harnessing the power of Big Data analytics and expanding information sharing.

LOE 3 centers on increasing network throughput and ensuring sufficient computing infrastructure. This LOE will generate the "always on, always available," end-to-end transport infrastructure necessary to meet growing and evolving capacity demands. It also will shepherd the transition from disparate data processing and storage solutions to an optimized and responsive global computing and storage infrastructure. Additionally, this LOE will implement a standardized suite of centrally managed end-user devices to improve functionality and to enable a common user experience.

LOE 4 focuses on delivering a universal suite of IT services, to include voice, video, data retrieval and sharing, and collaboration, from the enterprise to the end user. Modernized enterprise services such as these will provide the Soldier and business user the ability to work in diverse environments without needing to learn how to use these new services after each relocation to a new geographic location or organization. Additionally, common collaborative services will help enable live, virtual and constructive training, split-based operations and global collaboration among regionally aligned forces.

LOE 5 will concentrate on strengthening network operations. This includes establishing an information exchange specification

framework and simplifying the design, assembly, transport and stand-up of mission-scaled networks. This LOE will set the requisites to enhance spectrum monitoring, assignment and de-confliction. It also will facilitate central oversight of network assets and mission readiness, creating full network situational awareness; and improve incident response and cybersecurity management services for the operating force.

The Army Network Campaign Plan near-term implementation guidance details activities planned for fiscal years 2015 and 2016. The mid-term guidance focuses on network capabilities for FY 2017-21. Together, these documents provide the blueprint for synchronizing Army network requirements with our planning and programming. Today, I would like to highlight a few of our most important efforts, some of which were under way before the campaign plan was developed but all of which feed the ultimate objective of a unified, agile, robust and secure network that fulfills the needs of our Soldiers and their leaders.

Building the Joint Information Environment (JIE)

DoD is in the process of realigning, restructuring and modernizing how the department's IT networks and systems are constructed, operated and defended. The concept is called the Joint Information Environment and it improves in many ways from previous network constructs. Its foundation is an open architecture, defined standards and specifications, shared IT infrastructure, and common ways of operating and defending all DoD networks.

Common services are provided at the enterprise level, to include Identity Access Management (IdAM) and mission-unique capabilities supplied by the components. The end result will be a functionally optimized, secure, interoperable and resilient environment.

Army network modernization efforts are the most visible and advanced component of DoD's JIE initiative. For example, the DoD CIO has designated the Army's Joint Regional Security Stack (JRSS) architecture as the department's enterprise solution for network security. JRSS performs firewall functions, intrusion detection and prevention, enterprise management, and virtual routing and forwarding. The stacks have path diversity and eliminate critical failure points, which will help assure timely delivery of crucial information to warfighters around the globe. Pairing Multi-Protocol Label Switching (MPLS), a virtual traffic management system, with the stacks will make data move faster and improve command and control, thereby significantly reducing the chances of information being stalled or lost due to high volume and congestion. In addition, by moving each Service from its own security architecture to JRSS, DoD is substantially shrinking the attack surface and reducing its IT infrastructure inventory.

The Army is teaming with the Air Force and the Defense Information Systems Agency (DISA) to execute the migration to JRSS. Currently, JRSS implementation is ongoing at more than a dozen sites in the continental United States and overseas. Migration of operational traffic to JRSS has begun in Joint Base San Antonio and will continue

throughout the southwest and southeast regions of the continental United States. Overseas, the Department will add an additional JRSS installation and begin migration of operational traffic in Europe. In Southwest Asia, we will complete three sites over the next three quarters. Overall, we expect to have 24 sites worldwide that will process both unclassified traffic and 25 sites for classified traffic. This reduces the surface attack area from over 1,000 separate security access points to less than 50, dramatically improving the cybersecurity posture of the network.

The Joint Information Environment will rely heavily on cloud computing. In partnership with DoD, DISA, the National Security Agency and the other Services, the Army helped shape development of DoD's initial cloud security architecture. Moving to cloud-based solutions will enable the Army to better focus limited resources on meeting evolving mission needs. Over time, this will significantly boost IT operational efficiency, improve mission effectiveness and position the Army to more quickly adopt innovative and emerging capabilities. The Army currently is implementing the necessary modernization plans and crafting processes and procedures to leverage commercial cloud service providers approved by DoD and the Federal Risk and Authorization Management Program (FedRAMP). We are on track to formally release our cloud computing strategy in March 2015. We'll follow that strategy with a cloud computing policy to guide how and where we host our enterprise resource planning and other mission-critical systems, which will be restricted to DoD-owned facilities.

Unified Capabilities (UC) are another element of the Army's implementation of JIE. UC will provide real-time communications, to include voice, video and data, from the enterprise level in partnership with DISA. By centralizing the provision of these services and integrating them through a joint construct, users will get more capability more quickly – all the way down to the tactical edge. Additionally, UC will greatly enhance our voice, video and data security. Currently, not all of our communication media leverage DoD Public Key Infrastructure (PKI) to ensure confidentiality, integrity and availability. In contrast, UC will be fully integrated with DoD PKI. The Army and DoD also expect UC to reduce costs, as the Department will be able to take advantage of its enterprise buying power and to divest expensive legacy infrastructure.

The Army is working to converge the disparate Reserve, National Guard and Corps of Engineer networks into the larger Army network to leverage common infrastructure and gain efficiencies. This supports JIE's realignment and restructuring objectives in that it collapses separate networks into a single standards-based network in order to achieve improved security, situational awareness and operational flexibility.

While originally begun to fulfill Presidential and Office of Management and Budget mandates to reduce the federal IT infrastructure inventory, data center consolidation also supports the Army's move to the Joint Information Environment. By decreasing the number of Army-owned data centers and moving as much data and as many applications as practicable into joint Core Data Centers, we are greatly improving the availability of key information to all mission

partners. Fewer data centers also means less risk of compromise to DoD and Army information and networks. Additionally, once the process is complete, the Army should reap substantial cost savings. The DoD CIO has directed that the Services close 60 percent of their data centers by FY18. As of the beginning of February, the Army had closed 305 data centers, which is 40 percent of our goal. I would like to note that budget constraints would adversely affect the Army's ability to achieve full compliance with this presidential initiative to cut operating costs and improve security and infrastructure efficiencies.

To take advantage of everything the JIE offers, the Army is expanding its infrastructure capacity – that is, the amount of traffic our network "pipes" can handle. By the end of FY16, the Army network backbone, which connects installations to the DoD Information Network, will be increased to 10 gigabits per second (gbps) with the capacity to increase to 100 gbps in the future.

Everything the Army is doing at the enterprise level and to construct the JIE feeds directly into preparing and enabling our tactical forces. Perhaps most importantly, these efforts will bring expeditionary mission command to fruition, which in turn will make the Army more expeditionary and more effective on the battlefield. The basic concept of expeditionary mission command is to give commanders the ability to continuously inform and influence their forces through all operational phases, to include while at home station, during training center rotations, while en route to a real-world mission and once they hit the ground. They also will be able to leverage intelligence processing, exploitation and dissemination services.

Enabling Expeditionary Mission Command

The Army network enables expeditionary mission command. Corps and divisions will use their home station mission command center to effectively execute mission command from home station for a broad array of missions.

En route mission command capabilities provide uninterrupted mission planning, synchronization and situational awareness while in transit to the operational theater. Our units will maintain situational understanding and, with that real-time knowledge, conduct adaptive planning while still in the air. The Army is leveraging combat-proven technologies developed by the Special Operations community and the Warfighter Information Network – Tactical program to provide this critical capability to the Global Response Force.

Transportable Tactical Command Communications (T2C2) will provide small teams and company-sized units a robust voice and data capability immediately upon arrival. The T2C2 solution will come in two mobile, modular, and scalable variants, one to support initial-entry teams and a second to support early-entry command posts.

Greater integration between the enterprise and tactical networks will help reduce gaps in connectivity during different stages of operations and enable the use of expeditionary mission command supported by reach-back to strategic assets and information.

Protecting and Defending the Network

An agile, global network won't be of much use to the Army, however, if it and the information it carries are not secure and trusted. Protecting the network and information plays into every choice we make about architecture, capability and use. That said, I would like to highlight a few of our most important security-related endeavors.

The Army is aggressively transitioning to the new DoD certification and accreditation process, known as the Risk Management Framework (RMF). The RMF uses the security controls identified in the Committee on National Security Systems baseline and follows the processes outlined by DoD and the National Institute of Standards and Technology. Importantly, the RMF makes DoD requirements and processes consistent with the rest of the federal government's, enabling reciprocity. It also expands certification and accreditation beyond information systems to cover all information technology, including applications and industrial control systems. The RMF enables continuous system monitoring, as well, which will give us our security posture in real time.

The Army is actively pursuing ways to track and counter the insider threat as part of improving our defense posture. The federal government mandated implementation of network auditing and monitoring capabilities to deter, detect and prevent malicious insider activity on classified networks. The Services and agencies also were directed to establish a centralized analysis, reporting and response capability (i.e., analytics hub) to analyze the collected information. The Army Protection Program supports development of the technical requirements, deployment plan and

funding strategy for such a capability to cover all generating and tactical force networks. Our blueprint will facilitate the sharing of counterintelligence, information assurance, law enforcement, human resource, security and other related information.

Additionally, the Army is leveraging DoD's Host-Based Security System Device Control Module to restrict system access to peripheral and other removable storage devices and media, such as USB drives, MP3 players and CDs/DVDs. We also are using the DoD Insider Threat Detection Service, which utilizes the classified network-based Cyber Situational Awareness Analytic Cloud to detect potential malicious behavior, such as log tampering, data exfiltration and external web server attacks.

While automated tools are critical to better network security, they do not obviate the need for a first-class military and civilian cyber workforce. The Army is standing up a robust Cyber Mission Force that eventually will be composed of 41 teams and more than 1,800 military cyber personnel. The teams fall into five categories: national mission, combat mission, national support, combat support and cyber protection. As of the end of January, 24 teams had reached initial operating capability. We expect all 41 to be at full or initial operating capability by the end of FY16.

On the civilian side, the Army must bring the cyber workforce to a level of maturity that matches the recently established military Career Field 17 (CF17). That means developing a training pipeline; shaping the Army's talent management strategy to meet the increasing demand for a

credentialed civilian cyberspace workforce; and promoting Army efforts to unify and cohesively manage the civilian cyberspace workforce across the entire DoD. Potential models for civilian cyber talent management include: position identifiers similar to the acquisition workforce management process; a new Cyber Career Path that draws in cross-disciplinary occupational series from other career programs; and/or a new Office of Personnel Management cyber designation that would offer incentive pay and equity across agencies.

The CIO/G-6 is supporting an overall effort to build the Army's civilian cyber cadre. Last month, we initiated two planning teams. Among their tasks is defining work roles and competency/training requirements for the civilian workforce; and identifying the composition and scope of cyber-related positions, to include nine series residing in seven Army Civilian Career Programs (Information Technology, Telecommunications, Electronics Engineer, Computer Engineer, Computer Scientist, Intelligence Operations, Security, Criminal Investigation and Operations Research). Two more planning teams will start work in the June 2015 timeframe. One will focus on building a common framework among the seven Career Programs to manage the human resources life cycle of civilian cyber workforce. The other will integrate Army efforts into a federal framework and seek formal recognition of the civilian cyber workforce from the Office of the Secretary of Defense and the Office of Personnel Management to address occupational series, special pay, hiring flexibilities, and incentives.

FY16 Budget Request

The Army's FY16 IT budget request totals $9.1 billion and emphasizes the initiatives and programs just described critical improvements to cyberspace operations, cyber mission forces, core mission services, IT infrastructure, training and readiness. The request focuses on thorough modernization of the institutional network infrastructure so that we can take full advantage of warfighter and business technology advances. Partnering with DISA and our sister Services, with the requested funding in FY16, we will be able to make substantial progress in the transition from our disjointed legacy systems to a unified, more secure and capable network. Army users and our mission partners will reap tangible benefits as bandwidth expands, security is strengthened and enterprise services and applications come online. Additionally, FY16 network infrastructure upgrades will ensure that the Army is positioned to support cloud-based enterprise business systems and the adoption of Unified Capabilities.

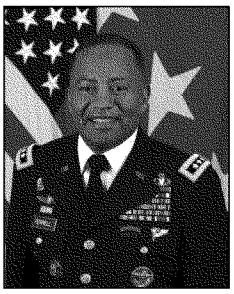
The Army has achieved significant cost savings and cost avoidance as a result of information technology management reforms in FY15 and leveraging Better Buying Power 3.0. Efficiencies identified are a result of deliberate reforms of IT governance structures: offering of flexible IT government contracts, consolidated purchases (bulk buys), issuance of standards, and maximizing the use of enterprise license agreements to achieve a single-interoperable secure network for deployment of information technology to modernize the network.

I know sequestration remains a topic of interest and the committee has asked about the impact of funding cuts. As General Odierno testified in January, under sequestration the Army would have to reduce spending

on network services and information insurance by almost $400 million in FY16. This would impact the Army's ability to sustain baseline network operations, which could, in turn, affect training, readiness and daily business activities. It also could impact our ability to maintain network security, which could create cyber vulnerabilities.

In closing, I would like to thank the committee for their support and the opportunity to appear today and discuss the importance of the Army network and information technology efforts. Information technology and the network are critical to the Army. Congressional support to our modernization efforts will ensure we can replace aging infrastructure, improve security through reducing access points and consolidate the Army's multiple networks into a single, seamless network that enables integrated strategic and tactical operations. It is imperative we deliver the network at the point of need, with the right bandwidth capacity, services and security to remain the world's preeminent land force.

I look forward to your questions.



Lieutenant General Robert S. Ferrell
Army Chief Information Officer/G-6

Lieutenant General Robert S. Ferrell became the Army CIO/G-6 on December 23, 2013.

As the CIO, Lieutenant General Ferrell reports directly to the Secretary of the Army, setting strategic direction and objectives for the Army network and supervises all Army C4 (command, control, communications, and computers) and IT functions. He oversees the Army's $10 billion IT investments, manages enterprise IT architecture, establishes and enforces IT policies, and directs delivery of operational C4IT capabilities to support warfighters and business users. As the G-6, he advises the Chief of Staff of the Army on the network, communications, signal operations, information security, force structure and equipping.

Lieutenant General Ferrell, a native of Anniston, Alabama, enlisted in the Army and attained the rank of Sergeant. He completed his undergraduate degree at Hampton University and was commissioned in August 1983, as an Army Signal Corps Officer. He holds a Master of Science Degree in Administration from Central Michigan University and a Master of Science Degree in Strategy from the Army War College.

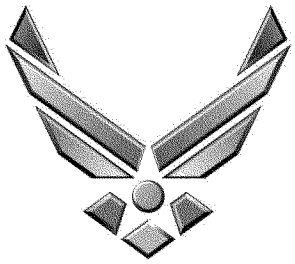
Throughout his career, he has served in Army units in the United States, Korea, and Europe and has deployed to Bosnia and Iraq. In addition to traditional company and field grade level assignments, he has commanded at every level from platoon to Army major subordinate command.

His principal staff assignments have been as Operations Officer and Communications-Electronics Officer, 2nd Battalion, 7th Special Forces Group (Airborne); Captain Assignments Officer, Signal Branch Army Personnel Command; Aide-de-Camp to the Secretary of the Army, Pentagon; Assistant Division Signal Officer, 82nd Airborne Division; Executive Officer, 82nd Signal Battalion; Operations Officer, 7th Signal Brigade, 5th Signal Command and Aide-de-Camp to the Commanding General, V Corps, United States Army Europe and Seventh Army, Germany; Military Assistant to the Executive Secretary, Office of the Secretary of Defense, Pentagon; Military Assistant to the Director, Program Management Office, Coalition Provisional Authority, OPERATION IRAQI FREEDOM, Iraq; Chief, Programs Division, Office of the Chief of Legislative Liaison, Pentagon; Army Senior Fellow, Council on Foreign Relations, New York; Director, Army Modernization, Strategic Communication, Army Capabilities Integration Center-Forward, Army Training and Doctrine Command, Pentagon; and Director for C4 Systems, United States Africa Command, Germany.

He commanded A Company, 426th Signal Battalion, 35th Signal Brigade, XVIII Airborne Corps; 13th Signal Battalion, 1st Cavalry Division and OPERATION JOINT FORGE, Tuzla; 2nd Signal Brigade, 5th Signal Command, United States Army Europe and Seventh Army, Germany; and Communications-Electronics Command, Aberdeen Proving Ground.

Lieutenant General Ferrell has earned numerous awards and decorations, most notably, the Defense Superior Service Medal (2nd Award); Legion of Merit (3rd Award); Bronze Star Medal; Meritorious Service Medal (6th Award), Army Commendation Medal (6th Award), and Army Achievement Medal (2nd Award).

United States Air Force



Presentation

Before the House Armed Services
Subcommittee on Emerging Threats
and Capabilities

Information Technology Investments and Programs: Supporting Current Operations and Planning for the Future Threat Environment

Statement of
Lieutenant General William J. Bender
United States Air Force
Chief, Information Dominance and
Chief Information Officer

February 25, 2015

INTRODUCTORY COMMENTS

Good afternoon Mr. Chairman, Ranking Member, and distinguished Members of the Subcommittee. Thank you for this opportunity to testify before the Subcommittee this afternoon on information technology (IT) investments and programs. I am Lt Gen Bill Bender, the United States Air Force Chief, Information Dominance and Chief Information Officer. My office is responsible for ensuring the United States Air Force has developed the governance, guidance, policies, and workforce to allow for the information access, secure communication networks, and decision support tools needed to provide mission assurance in support of the Air Force's five core missions. Our primary mission is to confront and overcome the challenges in defending, while simultaneously leveraging, cyberspace to affect mission assurance. In the first five months in this position, I've decided to act upon my responsibilities by focusing upon four major lines of effort: enhancing cybersecurity, advancing the Joint Information Environment (JIE), developing the Communications and Cyber workforce by transforming career field development, and operationalizing Chief Information Officer authorities. Information technology, including cyberspace, is at the core of what my office governs, leads, and manages each day. I'd like to describe my lines of effort, their relevance to IT within the Air Force, and the critical role they have in assuring the five core missions the United States Air Force must accomplish successfully.

Enhancing Cybersecurity

Freedom of action in cyberspace through the application of mission assurance is a prerequisite for successful Air Force core mission execution. Obtaining and maintaining freedom of action prevents the enemy from effectively interfering with operations. It also

allows the Air Force to deliver more combat power by exploiting cyberspace's unique characteristics. The Air Force will integrate cybersecurity throughout the lifecycle of weapon system development in all mission areas and will focus efforts on keeping information secure. As a man-made entity, cyberspace is fertile ground for game-changing innovation; innovative ideas of our Airmen will be rapidly identified, vetted, funded, and implemented across the Air Force to maximize potential and meet future Air Force needs. Cybersecurity is necessary to achieve these needs.

Thus, cybersecurity is at the forefront of my priorities for IT within the Air Force. I am working to move the Air Force toward overcoming the challenges posed by our complex systems and networks and confronting cyberspace vulnerabilities. The Internet Society, a non-profit entity dedicated to keeping the internet as an open platform, estimated that in 2015 there will be three billion internet users worldwide. CISCO Systems, Inc., estimates there will be 15 billion internet-connected devices by this year. Each internet connected person and device represents a potential vulnerability to cyberspace. We must understand and confront the reality that a contested cyberspace affects our wartime operations and opens our aircraft and systems to vulnerabilities.

To confront this issue, I have convened, under the direction of the USAF Chief of Staff, the Cyber Task Force. Several Air Force organizations are working this issue, but what has been missing is an enterprise level coordination and approach to provide solutions. This task force teams us with our operations and intelligence teammates to integrate efforts across the Air Force and focus on concrete action steps to mitigate our risks within cyberspace. This task force will not only work to define the threats and vulnerabilities, but also provide a risk management strategy and the needed actions and investments to

implement them. The focus of this task force is to recommend steps to provide mission assurance in a contested environment: mission assurance, not system assurance.

Joint Information Environment

Cybersecurity also drives one of my other lines of effort: enhancing the Joint Information Environment. The Air Force will achieve greater collaborative efficiency across the DoD and with external mission partners by bringing Air Force IT architectures, systems and processes into compliance with the Joint Information Environment (JIE). We will leverage opportunities to manage information and develop a data management plan to ensure data veracity as well as the accessibility of information to mission users. This ambitious effort to align, constructs, and defend our networks aims to provide better information access for users. JIE will help deliver mission assurance and provide warfighters and our mission partners a shared IT infrastructure. It will leverage networks with common configurations and enterprise services within a defendable single-security architecture. JIE will help protect the integrity of information and increase the ability to respond to security breaches across the enterprise. Air Force core missions benefit from all of these actions through greater operational and technical resilience, improved interoperability and effectiveness, enhanced integration across information systems, faster capability delivery, prioritized secure capabilities, and reduced costs. Ultimately, field commanders will benefit the most from JIE; they will be able to integrate information technologies, operations and cybersecurity to meet today's fast-paced operational conditions.

Now is the right time for the Air Force to become a full, aggressive partner in ensuring progress towards this concept. This is a multi-service effort and the DoD CIO is

moving forward; however, we must ensure every Service is committed to the effort, including in their budget, and that JIE is aligned in their Service priorities.

Revolutionize IT/Cyberspace Workforce Development

Another focus area is the need to completely transform the development of our IT and cyberspace workforce. The Air Force will continue its long-standing tradition of fostering and promoting innovation, especially in leveraging cyberspace. We will improve our policies and training and education programs to foster a workforce of highly skilled and qualified Cyber-Airmen who execute, enhance and support Air Force core missions. Cyber-Airmen will be experts not only in cyberspace, but in the core missions to which they contribute. Cyber-Airmen will also receive specialized training to ensure they are proficient within the system and platform to which they are assigned. This includes continuous training and education throughout their careers to allow for the development of the advanced skill sets needed to operate and defend cyberspace mission systems. We will also focus on the education and training of our civilian personnel to better leverage their skills and foster collaborative workplace environments. Additionally, the Air Force will recruit science, technology, engineering, and mathematics (STEM) professionals to lead and operate within the cyberspace career field. We will also educate and train personnel outside of the cyberspace community to gain the best understanding of how cyberspace contributes to the overall Air Force mission.

Our readiness is critically dependent upon a properly trained, equipped, and funded workforce. We will work with DoD efforts to recruit, train, and retain those with the necessary skillsets to meet the IT and cyberspace challenges of the 21st century.

Operationalizing CIO Responsibilities and Authorities

This office has taken great strides in aligning authorities and the organization to support warfighting integration across all Air Force mission areas. We are integrating cyberspace strategy, policy and programming across the mission areas, Air Staff, and lead command units in the field. This effort aims to provide the right information to the right people at the right time. By fostering the flow and sharing of information, we are working to improve combat execution.

Investments and spending on cyberspace capabilities across the Air Force must be fully transparent and aligned with supporting mission assurance. Improved spending alignments will provide additional resources for modernization and further innovation. My office will assist programs that acquire cyberspace and IT capabilities at earlier and more varied stages of the acquisition process than it does at present. This will improve responsiveness, unity of effort, and the Air Force's ability to implement best practices in cyberspace/IT investments.

However, we must understand that IT investments are the price of doing business in the 21st century. We cannot delay investments and deliver outdated technology and capabilities to the field. We must work to refine acquisition processes to make more timely decisions and deliver the latest capability to the field.

For example, the tools involved in reporting financial data are complex and mystifying. We manually input information into one repository, upload spreadsheets into another system, and enter additional data into a third database for the AF Corporate structure. The Air Force submission process is a maze of steps across four organizational hierarchies. The Presidential Budget cycles involve several actions and many actors over a short timeline.

These processes are dependent upon dissimilar systems from the respective services to those at the OSD and DoD levels. In order to deliver current IT capabilities to the field, these complicated processes need an overhaul. A roadmap and plan for this OSD and Service integration activity needs to be accomplished. The output would be a more expeditiously reported IT Budget with greater fidelity.

My office is fully aligned with executive measures to improve IT management and acquisition. Effective federal IT acquisition requires thorough knowledge of the federal acquisition system, a deep understanding of commercial IT capabilities, and the unique challenges inherent to successfully delivering large IT programs within limited time constraints. Our office is committed to the development of project management (PM) and IT skills within the workforce; and we're working to determine the proper placement, certification, and use of personnel as program managers of IT systems.

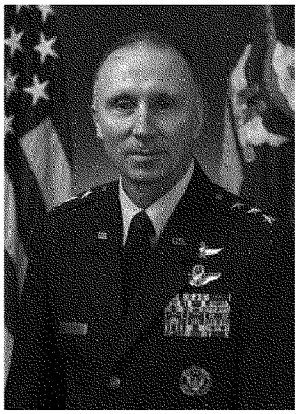
Conclusion

Delivering IT and cyber capabilities to the warfighter so they can provide mission assurance is absolutely critical to our national security. Our lines of effort outlined above will help deliver personnel, capabilities, and resources that provide greater mission assurance. We look to provide needed IT and cyber improvements and make the most efficient use of financial resources. I thank you for the opportunity to address this subcommittee. I thank you for your interest in, and leadership on, these critically important IT and Cyber-related issues, and I look forward to your questions.

BIOGRAPHY

UNITED STATES AIR FORCE

LIEUTENANT GENERAL WILLIAM J. "BILL" BENDER



Lt. Gen. William J. "Bill" Bender is the Chief, Information Dominance and Chief Information Officer, Office of the Secretary of the Air Force, the Pentagon, Washington, D.C. General Bender leads three directorates and supports 54,000 cyber operations and support personnel across the globe with a portfolio valued at $17 billion. He has overall responsibility of the Air Force's Information Technology portfolio as the senior authority for Information Technology investment strategy, networks and network-centric policies, communications, information resources management, information assurance, and related matters for the Department of the Air Force. As Chief Information Officer, General Bender provides oversight of portfolio management, delivers enterprise architecture, and enforces freedom of information act and privacy act laws. He integrates Air Force warfighting and mission support capabilities by networking air, space, and terrestrial assets. Additionally, he shapes doctrine, strategy, and policy for all cyberspace operations and support activities.

General Bender was commissioned in 1983 after earning a Bachelor of Engineering degree from Manhattan College. He has held staff assignments at Air Mobility Command, Headquarters U.S. European Command and Headquarters U.S. Air Force. His commands include an airlift squadron, an operations group, an air refueling wing, an airlift wing, and the U.S. Air Force Expeditionary Center. He has also served as Vice Commander of the 21st Expeditionary Mobility Task Force. Prior to his current assignment, he was the Deputy Chief, Office of Security Cooperation-Iraq, Baghdad, Iraq.

The general is a command pilot with more than 4,000 hours in the T-37, T-38, C/KC-135A/E/R, KC-10, EC-18B, E/KE-3A/B, C-141B, C-17A, C-130E and C-130J.

EDUCATION

1983 Bachelor of Engineering degree (electrical), Manhattan College, N.Y.
1986 Squadron Officer School, Maxwell AFB, Ala.
1989 Master of Arts degree in business administration, Embry-Riddle Aeronautical University, Fla.
1995 Air Command and Staff College, Maxwell AFB, Ala.
1996 Armed Forces Staff College, Norfolk, Va.
1999 Air War College, by correspondence
2002 Master of Arts degree in national strategic studies, Army War College, Carlisle Barracks, Pa.
2005 Senior Leaders Executive Course, John F. Kennedy School of Government, Harvard University, Cambridge, Mass.
2006 Senior Leaders Executive Course, Center for Creative Leadership, Greensboro, N.C.
2010 Senior Managers in Government Course, John F. Kennedy School of Government, Harvard University, Cambridge, Mass.
2011 Joint Flag Officer Warfighting Course, Maxwell AFB, Ala.
2012 Combined Force Air Component Commander Course, Air University, Maxwell AFB, Ala.

ASSIGNMENTS

1. December 1983 - November 1984, student, undergraduate pilot training, Vance AFB, Okla.
2. May 1985 - January 1989, KC-135 flight commander, Loring AFB, Maine
3. January 1989 - September 1992, wing executive officer, Wright-Patterson AFB, Ohio
4. September 1992 - August 1994, flight test assistant operations officer, Tinker AFB, Okla.
5. August 1994 - June 1995, student, Air Command and Staff College, Maxwell AFB, Ala.
6. July 1995 - August 1997, joint staff officer, Current Operations (J33), Headquarters U.S. European Command, Stuttgart, Germany
7. August 1997 - February 2000, Operations Officer/Commander, 4th Airlift Squadron, McChord AFB, Wash.
8. February 2000 - July 2001, special assistant to the Commander, Air Mobility Command, Scott AFB, Ill.
9. July 2001 - June 2002, student, Army War College, Carlisle Barracks, Pa.

10. September 2002 - May 2004, Commander, 437th Operations Group, Charleston AFB, S.C.
11. May 2004 - March 2005, Vice Commander, 21st Expeditionary Mobility Task Force, McGuire AFB, N.J.
12. March 2005 - July 2006, Commander, 319th Air Refueling Wing, Grand Forks AFB, N.D.
13. July 2006 - December 2007, executive officer to the Deputy Commander, Headquarters U.S. European Command, Stuttgart, Germany
14. December 2007 - July 2009, Commander, 86th Airlift Wing, Ramstein AB, and Commander, Kaiserslautern Military Community, Germany
15. August 2009 - October 2010, Director, Warfighter Systems Integration, Office of Information Dominance and Chief Information Officer, Office of the Secretary of the Air Force, the Pentagon, Washington, D.C.
16. October 2010 - July 2013, Commander, U.S. Air Force Expeditionary Center, Joint Base McGuire-Dix-Lakehurst, N.J.
17. July 2013 - September 2014, Deputy Chief, Office of Security Cooperation-Iraq, Baghdad, Iraq
18. September 2014 - present, Chief, Information Dominance and Chief Information Officer, Office of the Secretary of the Air Force, the Pentagon, Washington, D.C.

SUMMARY OF JOINT ASSIGNMENTS
1. July 1995 - July 1997, joint staff officer, Current Operations (J33), Headquarters U.S. European Command, Stuttgart, Germany, as a major
2. July 2006 - December 2007, executive officer to the Deputy Commander, Headquarters U.S. European Command, Stuttgart, Germany, as a colonel
3. July 2013 – September 2014, deputy chief, Office of Security Cooperation-Iraq, Baghdad, Iraq, as a major general

FLIGHT INFORMATION
Rating: command pilot
Flight hours: more than 4,000
Aircraft flown: T-37, T-38, C/KC-135A/E/R, KC-10, EC-18B, E/KE-3A/B, C-141B, C-17A, C-130E and C-130J

MAJOR AWARDS AND DECORATIONS
Distinguished Service Medal
Defense Superior Service Medal with oak leaf cluster
Legion of Merit with two oak leaf clusters
Defense Meritorious Service Medal
Meritorious Service Medal with two oak leaf clusters
Aerial Achievement Medal with oak leaf cluster
Air Force Commendation Medal with oak leaf cluster
Air Force Achievement Medal with two oak leaf clusters

EFFECTIVE DATES OF PROMOTION
Second Lieutenant May 22, 1983
First Lieutenant May 22, 1985
Captain May 22, 1987
Major March 1, 1994
Lieutenant Colonel Jan. 1, 1998
Colonel Aug. 1, 2002
Brigadier General Sept. 26, 2008
Major General Oct. 14, 2011
Lieutenant General Sept. 19, 2014

(Current as of February 2015)

STATEMENT

OF

DR. JOHN ZANGARDI
ACTING DEPARTMENT OF THE NAVY CHIEF INFORMATION OFFICER
AND
DEPUTY ASSISTANT SECRETARY OF THE NAVY FOR
COMMAND, CONTROL, COMMUNICATIONS, COMPUTERS, INTELLIGENCE,
INFORMATION OPERATIONS AND SPACE

BEFORE THE

SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

OF THE

HOUSE ARMED SERVICES COMMITTEE

25 FEBRUARY 2015

NOT FOR PUBLICATION UNTIL RELEASED BY
HOUSE ARMED SERVICES COMMITTEE
SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

Introduction

Good afternoon Mr. Chairman and distinguished Members of the Subcommittee. Thank you for this opportunity to testify before the Subcommittee today on information technology (IT) modernization and policy. I am Dr. John Zangardi, the Department of the Navy's (DON) acting Chief Information Officer (CIO) and the Deputy Assistant Secretary of the Navy for Command, Control, Computers, Communications, Intelligence, Information Operations and Space (DASN C4I & Space). I will address current DON enterprise (the Navy (USN)/Marine Corps (USMC) enterprise) efforts to achieve network command and control (C2), interoperability and agility in meeting current and future threats, as well as future efforts and their related challenges. As acting DON CIO, I strive to ensure continued technical superiority across the DON by working with all stakeholders, to include the Fleet, acquisition, and requirements communities to counter advancing threats. I never lose sight of the fact that our primary focus is how to best support the Warfighter.

It is important that the Department never lose sight of the money - from either the Warfighter or Taxpayer perspective. Under the Next Generation Enterprise Network (NGEN) contract, the DON leveraged the natural forces of competition to save more than $1.2B over the FYDP to operate the Navy Marine Corps Intranet (NMCI) network. We are working to maximize other cost savings across the DON enterprise via Data Center Consolidation (DCC) efforts. Executing system and application consolidations into Navy Enterprise Data Centers (NEDCs), Marine Corps Enterprise Information Technology Services (MCEITS), and other government and commercial data centers will standardize and reduce the DON Information Technology (IT) footprint, achieving financial efficiency and increasing overall cyber security posture.

To this end, the DON is fully supportive of the Department of Defense Joint Information Environment (JIE) initiative or Mission Partner Environment (MPE) initiative. A key MPE cornerstone is the Joint Regional Security Stacks, or JRSS. JRSS are regionally based, centrally managed rack of servers, switches, and other equipment that will help to ensure that the Department's facilities use the same security architecture in order to move toward MPE. The Navy is leveraging NMCI and the Marine Corps Enterprise Network (MCEN) for alignment to and development of the JRSS architecture, foundational to the DoD's Single Security Architecture (SSA) and continuing to inform development of / align to the MPE construct.

Speed to market is critical. Acquisition cycle time must be considered in program formulation to make informed tradeoffs with cost and requirements, enabling DON leadership to balance risks and tailor programs accordingly. I believe our business processes must be designed to drive effectiveness and efficiency in. I will add that some degree of acquisition reform focused on reducing bureaucracy is necessary to reduce time to warfighter for critical IT systems. It is critically important that an environment that cultivates innovation be fostered. With future defense budgets stagnant or declining, innovation will be the competitive edge for our Navy and Marine fighting forces.

How do we foster an environment of innovation? We do it by encouraging and listening to those closest to the challenge. The DON is developing an Innovation Cell, the objective of which will be to take these new ideas from industry and quickly evaluate them against our needs. We want to decrease the time it takes to get the very best ideas into production and in the hands of Sailors and Marines. An excellent example of this includes our mobility effort, which will eventually transfer approximately 25,000 enterprise Blackberry users to smart devices such as iPhones and Android phones. We were able to start from zero to delivery of first mobile phone units in less than 4 months, which, in our world, constitutes light speed.

I also believe we have a great deal to learn from our Industry Partners. They are out front on IT - this is a fundamental shift in "culture" if you will, from the past paradigm on tactical aircraft, ships and other weaponry. The DoD drove those Major Weapon System requirements; with regard to IT, that is simply not the case. Unfortunately, for IT procurements, our acquisition system and business processes still speak to the procurement of Major Weapon Systems. Industry tended to adopt the federal government's business construct, even if not necessarily the most efficient. What we have come to learn is that the Major Weapons Systems Acquisition Model does not "fit" with today's Industry's IT procurement model, which is predominantly driven by speed to market. Today's industry leaders in IT are not inclined to modify their business model to fit ours – the DoD is but a small percentage of their overall business base. This makes IT procurements all the more challenging. We realize there are some things that cannot be avoided in contracting with the Government, and we are working with Industry to identify those and strike a balance with respect to the best of breed business practices that can be employed to benefit of us both. Working together, DoD and the Services can also seek to leverage their

presence in market segments where they do have more leading edge experience, such as cybersecurity, mobile communications and IT service contracting.

Fiscal Year (FY) 2016 budget request for information technology programs

The FY 2016 IT program budget places priority on emerging capabilities in the cyber and electronic warfare efforts and supports a more seamless environment while accounting for the unique differences of the afloat and expeditionary environments. Afloat, the Consolidated Afloat Networks and Enterprise Services (CANES) program continues the transition from legacy IT21 networks to consolidated afloat networks and enterprise services. Ashore, the NMCI and the MCEN form the foundation for DON's vision and strategy for network consolidation, that will be interoperable with and capable of leveraging other Department of Defense provided Net-Centric Enterprise Services. While often arduous, our existing efforts have resulted in a more consolidated and secure IT environment.

Our planned efforts will build upon that success to increase cybersecurity, "right size" our enterprise and position the Department to implement new technologies as appropriate. Efforts such as the inclusion of the Navy's Outside the Continental United States (OCONUS) network, ONE-NET into NMCI, Navy DCC and MCEITS will accelerate the consolidation of our environment. This will enable us to more expeditiously and completely implement initiatives in data strategy, cloud and mobile computing and position the Department to align with the DoD's MPE initiative.

Afloat Networks

The Consolidated Afloat Networks and Enterprise Services (CANES) program replaces existing afloat networks and provides the necessary infrastructure for applications, systems, and services required for the Navy to dominate the cyber warfare tactical domain. CANES achieved its Initial Operational Capability (IOC) in USS MCCAMPBELL (DDG 85) in October 2013. It is currently installed in seventeen ships; including one aircraft carrier, one large deck amphibious ship and fifteen destroyers. Installations are ongoing on eleven other ships. Fully integrating Marine Corps warfighting and IT requirements into CANES is also a priority. Rigorous interoperability testing of Marine Corps applications with CANES enables Marine Corps Expeditionary forces to seamlessly embark in Navy Amphibious Ready Strike Groups, enabling successful global execution of integrated Navy/Marine Corps mission areas.

The FY 2016 budget places priority on emerging capabilities in the cyber and electronic warfare efforts so that we can continue to recruit and train top talent to form 40 cyber mission teams by the end of 2016. We also include funding for Operation Rolling Tide (ORT), which invests in enhancements to our existing legacy networks prior to their replacement with CANES. ORT provides cyber defense-in-depth including defensive solutions for ships, security improvements for our command and control networks, and the expansion of some of our defense initiatives to tactical IT systems.

The Navy is developing capabilities to deliver cyber effects from land and sea-based platforms. Additionally, the Navy has established Task Force Cyber Awakening (TFCA) with the intent of gaining a holistic view of cyber security risk across the Navy and aligning cyber efforts across our platforms and systems. TFCA is tasked to deliver fundamental change to Navy's organization, resourcing, acquisition and readiness by extending our cybersecurity apparatus beyond traditional IT to our combat systems, combat support and other information systems while aligning and strengthening authority and accountability. TFCA has formed four Task Groups (TG), each with representation from across the Navy and Marine Corps:

- TG Capabilities will look at major actions and assessments already underway or recently completed and will prioritize investments to ensure that we are taking the right steps in the near-term.
- TG CYBERSAFE will construct a program that is patterned after the SUBSAFE program. CYBERSAFE will apply to a hardened, very limited subset of components and processes and will include rigorous technical standards, certification and auditing.
- TG Navy Cyber Security will evaluate current authorities, methods and resources to identify enhancements required to ensure the application of rigorous technical standards, certifications and assessments across the Navy.
- TG Technical will support the other TGs and will be comprised of senior engineers from the systems commands to ensure that robust, common technical standards and authorities are in place to drive cyber programs and systems.

Ashore Networks

On June 27, 2013 the DON awarded the NGEN Enterprise Services and Transport Services contract after extensive acquisition planning and source selection evaluation. Simply

put, NGEN is a success story. The NGEN contract demonstrates continued innovation and exemplary acquisition practices. NGEN provides increased contract flexibility, Government oversight, plus Command and Control (C2), security and competition at a lower cost through a tailored acquisition approach. NGEN, the follow-on to the NMCI contract, provides network services to more than 800,000 DON users utilizing 400,000 workstations at over 2,500 locations across the continental United States, Hawaii and Japan. The NGEN contract manages the NMCI network, the largest and most secure Information Technology (IT) network within the DoD with an annual operating budget in excess of $1.3 Billion.

Promote Effective Competition. The NGEN competition saved $1.2B across the FYDP (FY15-FY19) as a Major Automated Information System (MAIS).

NGEN is the natural evolution of the DON Networking Environment. NMCI began as the aggregation of hundreds of disparate networks into a cohesive network with a common standard of service, common price and common security architecture. Under NMCI, the prime contractor was responsible for design, control and maintenance of the network. NGEN advances competition by ensuring government understanding of the network as a whole, as well as the underlying segments and services while allowing for the ability to adapt to changing environments. NGEN's flexibility will enable potential evolutions, such as the JIE, to be implemented without the burden of re-competing the entire contract. This increased competition will also drive future innovation and price reduction without sacrificing performance or security of the DON's network. Furthermore, in NGEN, the Government will serve as the design and technical authority, enhancing C2 functions and cost control.

Accomplished Seamless NGEN Transition Ahead of Schedule. As of October 1, 2014 the DON completed its transition of NMCI seats from the Continuity of Services Contract (CoSC) to the NGEN contract. The NGEN contract transition is a significant achievement in the evolution and delivery of the Navy and Marine Corps' enterprise network. I am pleased to report:

- The transition was completely transparent to our end-users and occurred with no disruption or loss of service.
- Through careful planning and solid teamwork between the Naval Enterprise Networks Program Office, Network Warfare Command and our prime contractor, the team successfully shaved 90 days off the transition timeline, which allowed the DON to start realizing a $20M a month savings three months ahead of schedule.

- The DON now has increased operational and cost insight that will inform network maneuver and guide investment decisions.
- Delivery of capability enhancements continued throughout the transition to include increased information assurance, eradication of Windows XP from the NMCI environment, and approval to introduce iPhone and Android options for mobile cellular users.

Improved Cyber Security. The NGEN contract incorporates Commercial Off-the-Shelf (COTS), Government Off-the-Shelf (GOTS) products and Non-Developmental Items (NDI) to the maximum extent possible. NGEN Increment 1 includes the full set of capabilities of NMCI, while increasing Government operational and design control of the networks and proactive enhancement of Information Assurance and Cyber Security (CS) services to meet evolving security requirements. This approach further ensures that the government understands the network as a whole as well as the underlying services, technologies and processes so that they may be enhanced to gain acquisition and operational flexibility. Where approved and funded, NGEN will continue to expand the network through the migration of legacy networks to the same capabilities, such as the Navy's Outside the Continental United States (OCONUS) network, ONE-NET.

ONE-NET

ONE-NET is the OCONUS Enterprise common computing environment that is preparing to improve network health and align with NGEN requirements for a single shore Navy Enterprise Network (NEN). ONE-NET will utilize program and architectural alignment through transition into NEN to maximize use of constrained resources and promote enhanced interoperability. ONE-NET will incorporate the functional requirements from the JIE while maintaining alignment with the Navy's planned transition into JIE.

Mission Partner Environment

The DON fully supports the DoD MPE. In our view, MPE will be instrumental to increasing network security through centralized software delivery and management. NMCI can provide lessons learned for MPE. The DON intends for NMCI and the MCEN to serve as our primary onramps into MPE, incorporating MPE technical standards through our network

technical refreshment processes as those standards are defined and made available. The DON plans to begin full participation and is intricately involved in understanding how MPE will be implemented in the U.S. Pacific Command Area of Responsibility (PACOM AOR). The DON plans to align with the JRSS version 2.0 beginning in FY 2018, which will match capabilities already implemented in the Navy and Marine Corps' existing enterprise networks. MPE or any future evolution of the network must account for the unique aspects of afloat and expeditionary forces.

Data/Mobility/Cloud Strategy

Last month, Secretary Mabus announced the establishment of the DON's Task Force Innovation to harness the creativity that our Sailors, Marines and civilian employees display every day in the execution of their duties for the benefit of the entire department. A central focus for the Task Force will be improving the way the DON makes use of its information. The large amount of data constantly being created by the Navy and Marine Corps – everything from acquisition program measurements to lessons learned from operations and deployments – has the potential to serve as the basis for the next great idea if it is available to the right minds at the right time, and the DON means to capitalize upon advances in computing power and analysis tools to gain greater advantage from the information it holds.

Some of the initiatives currently underway will significantly advance our effort. By placing our data where the right people can access it, and giving them better means to do so, we can unleash the creative power of our workforce. Our data center consolidation and application rationalization work, besides the security improvements and cost savings it will bring, is moving us toward our goal of a single integrated ashore infrastructure that will simplify access to authoritative data. The "anytime, anywhere" access we are trying to create requires more than an infrastructure, people need a means of gaining access. To that end, we are transitioning to the use of computers with native wireless capability and preparing to replace the portable devices our people currently use with industry standard smartphones and tablets that separate business from personal data to make our mobile workforce more effective. The young people entering the Services today have grown up with, and expect to use this technology. To continue to attract talent, we must be more technologically competitive. A very successful smartphone test begun last December is coming to completion, and we should have 25 thousand devices in use by the end of the Fiscal Year.

To realize the greatest benefit from our move to more capable devices, the DON also needs to take the fullest possible advantage of cloud computing technology. The DoD CIO released updated guidance on acquisition and use of cloud services last December, and we are working with DoD CIO, Defense Information Services Agency (DISA) and the other Services to develop concepts of operations, security strategies, and business processes for moving data into the appropriate mix of public and private clouds. One of the chief issues for us to resolve is the difference between the way services like cloud computing are procured by commercial entities, and the way we must do it, given Defense acquisition law and policy. We are anxious for the benefits promised by cloud computing, and are moving as quickly as possible. However, there are important contracting, as well as data and security considerations that must be worked through before we can accelerate the pace.

While there are challenges to overcome, these are changes we need to make to enable the innovation necessary to retain our advantage. We intend, as former Microsoft CEO Steve Ballmer once said, to use information technology to empower people to do what they want to do, to let them be creative and productive.

Data Center Consolidation

The principal aim of the DON's data center consolidation effort is to gain cost efficiencies while increasing Navy and Marine Corps efficiency and standardization and raising the department's overall security profile. This will be accomplished by decreasing overall data center facility footprint, increasing system virtualization, and maximizing use of commercial and government provided public and private cloud services, as appropriate, to host our data. While the Navy and Marine Corps will follow somewhat different paths, as dictated by Service requirements, we are working toward common outcomes. To date the department has closed over 50 Continental United States (CONUS) data center facilities and has targeted at least 79 more for closure, with several more facilities under review. The Navy intends to have no more than 28 CONUS Installation Processing Node (IPN)-sized data centers in operation and move as fast as practical to leverage commercial data centers by the end of 2019; the Marine Corps will continue to employ its private cloud.

Our data center consolidation targets are aggressive but we believe they are achievable, though we face significant challenges. One of the most difficult tasks will be completing the

rationalization of our systems and applications into an optimal portfolio. We've learned much on our data center consolidation journey; and just as importantly, we have identified what we don't know. The challenges are steep but so are the benefits. Finally, we must continue to mature DoD policy and contracting language for procurement of cloud services to fully realize the benefits cloud hosting can provide. DoD and the Services are working closely on these issues, and we are confident that they can be resolved.

Electromagnetic Spectrum

The recently concluded electromagnetic spectrum auction was far more successful than most predictions anticipated, garnering over $40 billion. Of that, the DON expects to receive $1.5 billion through the Spectrum Relocation Fund to cover the costs of migrating our systems out of the auctioned frequency bands. Spectrum-dependent systems are embedded in nearly every operational platform in our inventory, all contribute to our ability to maintain dominance across the range of operations, and they require access to spectrum to do so.

The loss of any spectrum impacts military programs and associated weapons systems, and the auction of 25 megahertz will affect systems ranging from ship-to-shore wideband transmission terminals to small-unmanned aerial systems. Displacing these systems into alternative spectrum modifies their performance because they must compete with systems already operating in a congested spectrum environment. The Services were permitted only a very compressed timeline to capture the full range of actions required to shift programs out of the auctioned frequencies. While we do not anticipate any loss of military capability at this time, we are concerned that the accelerated pre-auction timeline did not enable the deliberation required to fully understand potential engineering challenges or operational modifications associated with systems functioning in a different spectrum band. Any further loss of spectrum would be cause for great concern, and no additional relocations should be undertaken without deliberate, comprehensive study to ensure there will be no loss of military operational capacity and no impact to United States national security.

Better Buying Power and IT Acquisition Reform

Ability to Control Costs Through The Product Lifecycle. Unlike NMCI, which was awarded as a Commercial Acquisition, NGEN was awarded under negotiated contract

procedures allowing for future competition. This significant change gives the Government enhanced price insight when evaluating changes and price differentials for individual services, ensuring that decisions provide the most cost-effective support for operational conditions. The NGEN acquisition approach allows for evolutionary development and will iteratively analyze the needs, requirements and available resources for future NGEN increments using a spiral development and implementation process. Leveraging this in-depth knowledge of the network and a highly severable contract structure, the DON is now in a better position to re-compete portions of NGEN to access a much broader competitive landscape of products and companies including a contract requirement that 35% of the total value must be dedicated to small business concerns.

Incentivize Productivity and Innovation in Industry and Government. NGEN is leveraging an Award Fee (AF) structure and a shared savings approach to further reduce cost, ensure performance is maintained, and to smoothly transition NMCI services to NGEN. The AF pool is structured to incentivize exceptional performance in areas where it is difficult to objectively measure performance. The AF will be used to ensure seamless transition to the NGEN service delivery model, for effective dispute resolution between the government and contractor, to ensure adherence to the small business participation goals, and to ensure highly innovative technology refresh plans are implemented to continue to drive down government cost and increase network security without sacrificing performance. Modeled after a clause in the NASA ACES-II contract, the shared savings clause stimulates innovations and "good ideas" where the Government and the contractor share in the savings. Often this is a 50/50 share, but in NGEN this will be negotiated as part of each proposal.

IT Acquisition Workforce

The Navy is undertaking several initiatives to strengthen its IT Acquisition Workforce. Consisting of both military service members and members of our civilian workforce, the IT Acquisition Workforce is obtaining increased levels of certifications and training appropriate for both the changing Information Technology threat environment and the evolving acquisition guidance represented by the better buying power initiatives and changing DoD regulatory environment.

The Acquisition workforce itself is tracked at large scale against 5 specific goals: (1) certification of individuals to the appropriate level of qualifications for identified positions; (2) individual maintenance of expertise as represented by continuous learning requirements; (3) positional goals of filling what are identified as critical acquisition positions with qualified members (through membership in the Acquisition Corps); (4) completion of executive level Program Management training; and (5) support of identified programs with appropriately qualified experts through tracking of key leadership position fills. We have made steady progress against all five of these goals has been made over the last two years with each area trending upward.

Technical training continues to evolve, particularly in the area of Information Technology. The DoD Cybersecurity workforce is transitioning the inventory of required knowledge, skills and abilities (KSA's) to the National Incentive for Cybersecurity Education (NICE) Framework. Specific work is ongoing with the KSA's associated with the Cybersecurity Workforce, the IT Acquisition Workforce, and individual skill areas such as "Data Professional". In partnership with academic organizations (such as the UCSD San Diego Supercomputer Center), we are matching course work and workshops (such as "data analytics boot camps") with skills necessary for our government workforce.

Acquisition of new talent is also being pursued. The DON has the opportunity to promote our current and future programs; offer paid internships to college students; and most importantly, offer invaluable experience in the world's leading defense acquisition organization. The Navy is exploring various means to offer college juniors and seniors a start to a successful career in Navy Acquisition. In July 2014, the Navy began to define a strategy that would reinvigorate DON acquisition recruiting on college and university campuses. The foundation of this strategic pilot will be built upon the Pathways Internship Program (previously known as SCEP) that leverages the current HR system to hire rising college juniors at the GS-4 level to work at command headquarters during the summer and/or extended breaks. The program is being established for 24 months per Intern. After successful completion, Interns can be non-competitively converted to the Naval Acquisition Development Program at individual Systems' Commands within 120 days of graduation.

While we are exploring the aforementioned hiring innovations to reach the best and brightest in the IT market, Direct Hiring Authority and HR reforms are needed to compete with private industry employers.

Thank you for your time and attention to these matters.

Dr. John Zangardi, Ph.D.

Deputy Assistant Secretary of the Navy for Command, Control, Communications, Computers, Intelligence, Information Operations and Space
Assistant Secretary of the Navy
(Research, Development & Acquisition)

John Zangardi was appointed as Deputy Assistant Secretary of the Navy for Command, Control, Communications, Computers, Intelligence, Information Operations, and Space (DASN C4I/IO and Space) in March of 2011. In support of ASN (RD&A), Dr. Zangardi is the principal Department of the Navy advisor for C4I, IO, space (including space-related acquisition), business enterprise acquisition, and information technology and resources management. In his oversight role, he coordinates with key stakeholders to maximize alignment with Navy and Marine Corps needs.

He is a native of Scranton, Pennsylvania and a graduate of the University of Scranton. Dr. Zangardi was awarded a master of science degree from the Naval Postgraduate School and a doctorate from George Mason University.

Commissioned through the Aviation Officer Candidate School, he was awarded Naval Flight Officer wings in 1983. Operationally he served with Patrol Squadron 6, USS Abraham Lincoln (CVN-72), Patrol Squadron 8, and Patrol Squadron 26 as Commanding Officer. Ashore, his assignments include Patrol Wings Pacific, Joint Staff (J6) as Lead Budget Analyst, Navy Staff (N78) as Assistant for Programming and Budget, and Navy's Office of Legislative Affairs as Director for Naval Programs.

After leaving active duty, he was employed by BAE Systems Electronics and Integrated Systems operating group, Arlington, Virginia. He was assigned as Director for Maritime Systems and Requirements.

In January of 2008, Dr. Zangardi was selected for appointment to the Senior Executive Service (SES) with assignment as Deputy Director for Warfare Integration Programs (N6FB), within the Directorate for the Deputy Chief of Naval Operations Communications Networks (N6).

With the stand-up of the Deputy Chief of Naval Operations Information Dominance (N2/N6), he was assigned as Director for Program Integration and as Deputy to the Director for Concepts, Strategy, and Integration.

DRAFT
V 4.2 18 Feb 2015

STATEMENT BY

BRIGADIER GENERAL KEVIN J. NALLY
HEADQUARTERS UNITED STATES MARINE CORPS
DIRECTOR C4
DEPUTY DEPARTMENT OF THE NAVY
CHIEF INFORMATION OFFICER

BEFORE THE

HOUSE ARMED SERVICES COMMITTEE

SUBCOMMITTEE ON

EMERGING THREATS & CAPABILITIES

ON

"Information Technology Investments and Programs: Supporting Current Operations and Planning for the Future Threat Environment"

FEBRUARY 25, 2015

NOT FOR PUBLICATION UNTIL RELEASED BY THE SUBCOMMITTEE ON EMERGING THREATS & CAPABILITIES, HOUSE ARMED SERVICES COMMITTEE

DRAFT
V 4.2 18 Feb 2015

Director C4, DDoN CIO Marine Corps Congressional Testimony

Chairman Wilson and distinguished members of the Subcommittee, thank you for your support to your Marine Corps and the opportunity to appear before you today along with our counterparts and teammates.

The Marine Corps is the Nation's expeditionary force-in-readiness and is forward-stationed, forward-deployed and forward-engaged. We have this posture to be ready to fight tonight in any clime or place and partner with the Navy to come from the sea and operate ashore, alleviating dependence on fixed bases or facilities. As our Commandant has identified in his planning guidance, it is imperative on the battlefield that we assume the enemy will seek to compromise or degrade our ability to command and control and we should seek to reduce the dissimilarity between how we conduct ourselves in combat and garrison. Our readiness to fight is based on Five Pillars of Readiness, which consist of operational and foundational readiness across Force Structure, Unit Readiness, Capability to Meet Combatant Commanders Requirements, Facility Investments and Equipment Modernization. The common key enabler across these Pillars of Readiness is their requirement to exchange data, information and knowledge leveraging Information Technology (IT). Our warfighters require access to the right data at the right place at the right time. The demand for information will not tolerate a break in access. With the speed in which technology evolves today, we must continue to grow our IT capabilities throughout the entirety of the Marine Corps enterprise. Information must be available seamlessly through multiple mediums, from flag pole to fighting hole. Our end state is to enable command and control in a single information enterprise that supports the way the Marine Corps operates, which includes a range of missions from today's crisis response to supporting our Expeditionary Force 21 concept.

Unifying Our Network

Our single Marine Corps Enterprise Network (MCEN) will be our instantiation of the Joint Information Environment (JIE), and the MCEN Unification Plan (MCUP) is our plan to achieve it. This plan relies on leveraging Next Generation Enterprise Network, Secure Operational Network Infrastructure Capability, Marine Corps Enterprise Information Technology Services and Base Telecommunication Infrastructure programs of record to continue as currently proposed in the Fiscal Year 2016 Presidential Budget. Our main focus today is unifying our networks to securely and seamlessly connect deployed and engaged forces to Joint data, information and knowledge at the time they need it. Sustained investment will allow the Marine Corps to reduce legacy systems, maintain the momentum achieved to date in the MCUP and gain efficiencies.

As JIE continues to develop, the Marine Corps will analyze future capability, programming and resourcing implications and refine the plan as necessary. We are reviewing our MCEN defensive boundaries for instance, to determine what capabilities deployed Marine Air Ground Task Forces (MAGTFs) will require that the Joint Regional Security Stacks (JRSS) may not provide. The Marine Corps completely supports the JRSS effort and is preparing to evolve to JRSS 2.0 in Fiscal Year 2018 by beginning optical core upgrades and transitioning to Multiprotocol Label Switching in Fiscal Year 2016.

The Marine Corps' Fiscal Year 2016 Information Technology Budget of approximately $1.6 billion is focused on completing the modernization of the Government Owned and Operated Next Generation Enterprise Network taken back from Hewlett Packard in 2013, improvements to the Secure Internet Protocol Routed Network, modernization and sustainment of Common Aviation Command and Control System Increment 1 and consolidating key Marine Corps

applications into Marine Corps Enterprise Information Technology Services. The overarching theme of these initiatives is to ensure reliable access to persistently used information for our Marines at the point of need, ranging the entire operational spectrum. These key actions directly support the Marine Corps' Five Pillars of Readiness.

We also continue to innovate and look for further efficiencies through cloud and mobility efforts within the Marine Corps. Our Cloud Strategy supports the Commandant's priorities and focus areas, such as fiscal responsibility, expeditionary energy and green IT. The Marine Corps Cloud Strategy will reduce cost and save energy by consolidating and centralizing resources, including hardware, software, and licenses. This strategy also supports the Marine Corps Information Enterprise (MCIENT) by implementing seamless, mobile communications and knowledge/information management across the enterprise. The benefits of the Cloud Strategy include the realization of a single enterprise for the supporting establishment and forward deployed forces in a manner that is effective and efficient with respect to fiscal restraints, manpower sourcing and operational tempo.

The Marine Corps Cloud Strategy is rooted in the National Institute of Standards and Technology (NIST) Definition of Cloud Computing and the Federal Cloud Computing Strategy. The foundational enabler for the Marine Corps strategy is the Marine Corps Enterprise Information Technology Services (MCEITS), which establishes the Marine Corps' guidance for synchronizing current Marine Corps IT programs. The Cloud Strategy will ensure the Marine Corps complies with and aligns to federal requirements and guidelines by ensuring that IT services are distributed across the enterprise in fiscally and operationally efficient and effective manners.

The currently constrained budget environment requires us to balance fiscal responsibility with mission accomplishment. To align to DOD strategies and initiatives and in accordance with the MCIENT, the Marine Corps has begun consolidating data centers and executing our Cloud Strategy. With increasing mobile device capabilities, the Marine Corps recognizes the trend of evolving information needs across our operating environments and the need to provide an agile method of meeting those needs. The user requirement to access and share information from non-traditional workspaces will enable more efficient mission accomplishment. The ability to access, share and manipulate data and information from non-traditional workspaces will afford users with additional freedom of movement across an expanding information environment. The flexibility and ubiquitous ability to share information effectively will reduce the orientation and decision-making timelines, thereby affecting more rapid mission accomplishment.

IT Acquisition Process

The acquisition process continues to be deliberately procedure heavy and risk averse to ensure appropriate delivery of IT solutions. Statutory and regulatory changes will be required in order to enable responsiveness to emerging cyber threats and missions. Current IT acquisition processes do not adequately support the delivery tempo required for emerging IT and cyber solutions. The tempo at which IT solutions must be acquired to meet cyberspace operational mandates is occurring at a much greater pace, which creates tension within the acquisition process. We must strike a balance between rapid acquisition to meet emerging threats and changing operational demands and maintaining disciplined engineering rigor of enterprise networks.

Strengthening the IT Acquisition Workforce

The Marine Corps faces challenges with developing, hiring and retaining its cadre of experienced IT professionals. The surge in demand for experienced IT professionals has made it difficult for the Marine Corps to viably compete with the salary and benefit packages provided by private industry. This demand, coupled with downsizing of the acquisition workforce across the Department of Defense has led to increased attrition rates and significant increases in the quantity of vacancies in critical IT acquisition positions. The pace of IT innovation and the constantly evolving cyber threats has further compounded the challenge of accurately defining requirements, rapidly acquiring, and adequately sustaining secure, state-of-the-art IT systems that work seamlessly in joint and coalition environments.

Given the challenges identified, the Marine Corps has taken several steps to strengthen and augment its organic IT workforce. Specifically, the Marine Corps:

- Continues to seek and maintain professional certifications for employees operating within specific IT domains, such as information assurance management, in accordance with Department of Defense Directive 8570.

- Continues to provide resources for IT professionals to obtain advanced technical training courses to improve competencies in IT related fields.

- Improved its planning processes with Naval Warfare Centers and other Government research centers to improve reach-back access to qualified IT professionals to augment its organic IT workforce embedded within acquisition program offices.

- Actively recruits and develops its future cadre of information technology specialist, telecommunications specialists, computer scientists and engineering professionals as part of

various intern programs offered through the Department of Defense, with specific success noted through the Department of Navy intern program and the Science, Mathematics and Research for Transformation (SMART) program.

- Identified critical IT vacancies as a high priority for active job solicitations and hiring actions as authorized.

While these efforts have aided in reducing the impacts brought about by attrition losses, these challenges are likely to persist for the foreseeable future and may impact the Marine Corps' IT acquisition workforce.

Investment Review and Management Processes

To mitigate IT risk, and ensure compliance with laws and regulations, the Marine Corps Information Environment supports the Marine Corps goals and objectives, the CIO has input and authorities related to: (1) force development; (2) the Planning, Programming, Budgeting and Execution (PPBE) process; and (3) acquisition processes. Additionally, the Marine Corps currently conducts investment reviews using an Information Technology Steering Group, which evaluates current and future IT investments across the Marine Corps to ensure their alignment and performance to Marine Corps strategic priorities. The Marine Corps Information Technology Steering Group further reviews and assesses IT investments providing qualitative and quantitative input that influences acquisition and sustainment decisions.

Currently, efforts are underway to review the Marine Corps Chief Information Officer (CIO) role. Through strengthened authorities and process input, the CIO can deliver IT investment plans that generate cost savings/avoidance and provide assured capabilities with:

- Repeatable processes and enforcement mechanisms that eliminate duplicative and unnecessary IT capabilities.

- Enterprise IT services that align to strategic goals and objectives.

- Standardization of IT capabilities and governance across the Marine Corps Information Enterprise.

This effort increases involvement in IT investment decisions, to include providing the CIO additional authorities and responsibilities over contracts for IT capabilities and the certification of the accuracy of the risks associated with IT investments across the Marine Corps. In addition, the Marine Corps has realigned its requirements management process to take a more holistic view of force development activities. This realignment gives greater visibility to all aspects of Doctrine, Organization, Training, Materiel, Leadership, Personnel and Facilities that are required in delivering fully supported capabilities aligned to the Marine Corps strategic priorities.

Conclusion

The future operating environment will continue to stretch the employment capacity of the United States and require a force-in-readiness with global response capabilities. Declining budgets may result in further stretching of the force; however, the President's Budget supports the best balance of resources in support of achieving the Commandant of the Marine Corps' planning guidance. The Marine Corps will continue to be our Nation's force-in-readiness, ready to answer the call and fight tonight. We will ensure our IT investments and workforces are capable and trained to meet today's unpredictable and dynamic operating environment. Thank you for your support of our Marines and for the opportunity to represent our Corps today on these important topics.

Brigadier General Kevin J. Nally, Deputy Chief Information Officer (Marine Corps)

November 22, 2010

Brigadier General Kevin J. Nally is the Director for Command, Control, Communications, and Computers (C4), and the Department of the Navy Deputy Chief Information Officer for the United States Marine Corps.

Brigadier General Kevin Nally was commissioned a Second Lieutenant in the Marine Corps in May 1981, after graduating from Eastern Kentucky University with a Bachelor of Science in Agronomy and Natural Resources.

After completing the Basic School and Communications Officer Course, he was assigned to the 1st Marine Amphibious Brigade where he served as a Communications Platoon Commander for the Marine Service Support Group-37 and later as a Communications Platoon Commander for the Brigade Service Support Group. During this tour, Brigadier General Nally attended SCUBA School, Pearl Harbor where he served in an additional duty capacity as a search and rescue diver.

In 1985, he was reassigned to Marine Corps Recruiting Station, Los Angeles, Calif., where he served as an Officer Selection Officer.

In 1988, Brigadier General Nally attended Command, Control, Systems Course in Quantico, Va. After graduating in 1989, Brigadier General Nally was assigned to the 2nd Tank Battalion, 2nd Marine Division where he served as the Communications Platoon Commander during Desert Shield and Desert Storm. Following this, he was assigned to Communications Company, Headquarters Battalion, 2nd Marine Division as the Executive Officer.

In 1992, Brigadier General Nally was assigned as the Operations Officer, Recruit Training Regiment, Marine Corps Recruit Depot/Eastern Recruiting Region, Parris Island. In 1995, Brigadier General Nally was transferred to the 3rd Marine Division where he served as the S-6, then the S-3, and finally as the Executive Officer for the 4th Marine Regiment. In 1996, he served as the Commanding Officer, Communications Company, Headquarters Battalion, 3rd Marine Division.

In 1998, Brigadier General Nally was assigned as the Deputy Director, J6, United States Forces, Japan and completed a master's in information systems management.

From 2000 to 2002, Brigadier General Nally was the Commanding Officer of Support Battalion, MCRD/ERR, Parris Island. From May of 2002 to July 2003, Brigadier General Nally was the Director, Marine Corps Martial Arts Program.

Brigadier General Nally is a 2004 graduate of the Industrial College of the Armed Forces with a concentration in information strategy. Following this assignment, he served from 2004 until 2006 as the Deputy Director for C4, United States Central Command where he deployed twice in support of OIF/OEF. In 2006, Brigadier General Nally was transferred to Camp LeJeune, N.C., where he served as the II MEF AC/S G-6 and subsequently as the II MEF Chief of Staff. From 2007 until 2009, he served as the Commanding Officer, Marine Corps Communications-Electronics School in 29 Palms, Calif. He served as the AC/S, G-6, MCAGCC/MAGTF-TC from 2009 until 2010.

His personal decorations include the Defense Superior Service Medal, Legion of Merit, Defense Meritorious Service Medal, Meritorious Service Medal with two gold stars, the Navy/Marine Corps Commendation Medal with three gold stars, the Navy/Marine Corps Achievement Medal, and the Combat Action Ribbon.

DOCUMENTS SUBMITTED FOR THE RECORD

FEBRUARY 25, 2015

STATEMENT BY

VICE ADMIRAL TED N. BRANCH
DEPUTY CHIEF OF NAVAL OPERATIONS
FOR INFORMATION DOMINANCE (N2/N6),
DEPUTY DEPARTMENT OF THE NAVY (DON)
CHIEF INFORMATION OFFICER - NAVY,
DIRECTOR OF NAVAL INTELLIGENCE,
AND HEAD OF THE NAVY'S INFORMATION DOMINANCE CORPS

BEFORE THE

HOUSE ARMED SERVICES COMMITTEE

SUBCOMMITTEE ON

EMERGING THREATS & CAPABILITIES

ON

"Information Technology Investments and Programs: Supporting Current Operations and Planning for the Future Threat Environment"

FEBRUARY 25, 2015

Introduction

Good afternoon Mr. Chairman and distinguished Members of the Subcommittee. Thank you for this opportunity to provide written testimony for the record to the Subcommittee on information technology (IT) modernization and policy. I would also like to thank Dr. John Zangardi, the Department of the Navy's (DON) acting Chief Information Officer (CIO) and Deputy Assistant Secretary of the Navy for Command, Control, Communications, Intelligence and Space (DASN C4I & Space) for his testimony. My intent is to provide remarks complementary to his testimony.

I am Vice Admiral Ted Branch, Deputy Chief of Naval Operations for Information Dominance (N2/N6), Deputy DONCIO - Navy, Director of Naval Intelligence, and Head of the Navy's Information Dominance Corps. For this testimony and Subcommittee's interest, my written comments focus largely on my role as the Navy service's CIO. Like the Marine Corps, we have a uniformed service CIO below the Secretariat (DONCIO) level.

Before going too much further, it occurs to me that you may not be familiar with the term Information Dominance. We define Information Dominance as the operational advantage gained from fully integrating the Navy's information functions, capabilities and resources to optimize decision making and maximize warfighting effects.

In other words, it is about warfighting in the Information Age.

To accomplish our goals, we focus on three core capabilities: Assuring Command and Control, maintaining persistent Battlespace Awareness, and Integrating kinetic (missiles, warheads, etc.) and non-kinetic (cyber, electromagnetic spectrum) Fires.

With that as the basis for what we do, I will discuss five specific areas: The challenges that are inherently unique to the Navy; the Navy's roadmap to Risk Management Framework (RMF) implementation; our support to the Joint Information Environment (JIE), the Joint Regional Security Stack (JRSS) architecture, and Intelligence Community Information Technology Enterprise (IC ITE) efforts; Navy's role in information-age warfare; and our efforts in the cyber "fight for talent".

Navy Unique Challenges

So…what makes Navy unique? As many of you are aware, one-third of the Navy's Battle Force is operating at sea on any given day. This means that large portions of our tactical

afloat, OCONUS, and warfighting system networks are distributed on the front lines. Sustaining our global primacy requires that we dominate the battle space on, above, and below the surface of the sea, as well as in outer space. In this Information Age, we recognize and accept the premise that we must also successfully command, control, and fight our forces in the information domain, which includes the electromagnetic spectrum and cyberspace. This requires frequent and timely updates to our systems.

In this dynamic information dominance realm, operating in a benign afloat environment is challenging enough. In a communications denied or degraded environment, the complexity of fighting increases as does the difficulty of effectively maintaining command and control of our forces. With a large part of the Fleet operating forward, maintenance and modernization of our Command, Control, Communications, and Computer (C4) and cyber systems on the tactical edge is difficult. System configuration changes, security updates and patches must often be delayed until that unit is back in homeport for scheduled maintenance. As we try to pace the threat and technological advances, maintaining a highly capable Battle Force consisting of different high-optempo ship classes, variations among programs of record, and differing configurations is at best challenging. Additionally, with limited bandwidth available to our operating forces at sea and our focus on safely operating and fighting the ship, our quality of life initiatives – telephones, email, Facebook etc., – often take a backseat, impacting morale for both our Sailors at sea and their loved ones at home. Our Commanders must balance these priorities every day.

Risk Management Framework

The Navy is moving out with implementation of the Risk Management Framework (RMF). Phase I of implementation began 1 January 2015 and is in accordance with DoD CIO stated timelines for DoD implementation. Phase I includes all Navy IT assets currently accredited under the DoD Information Assurance Certification and Accreditation Process (DIACAP). Phase I will also utilize the current Operational Designated Accrediting Authority (ODAA) acting as the single Authorizing Official (AO) and the current Certifying Authority (CA) acting as the single Security Control Assessor (SCA). Phase II, which is still under development and will begin on or about July 2016, will incorporate all Platform IT (PIT): i.e, Weapons Systems; Industrial Control Systems (ICS); and Hull, Mechanical, and Electrical (HM&E) that were not covered under the previous Cybersecurity Accreditation policy. Both

Phase I and Phase II will be completed by October 2017, leaving Navy 100% complete with our implementation.

JIE, JRSS and IC ITE Efforts

The Navy is fully onboard with DoD's effort to consolidate individual service, component, and agency IT infrastructures into the Joint Information Environment (JIE). This is largely a shore-based infrastructure, and Navy's responsibility extends to the tactical edge at sea. JIE capabilities will be provided to all authorized Navy personnel afloat, ashore, and aloft by means of the following: (1) the Next Generation Enterprise Network (NGEN)/OCONUS Navy Enterprise Network (ONE-NET) and Navy Enterprise Data Center Consolidation ashore; and (2) the Consolidated Afloat Networks and Enterprise Services (CANES) network, Automated Digital Network System (ADNS) Increment III router, Navy Multiband Terminal (NMT) transceiver, and such hosted and connected applications as the Global Command and Control System Maritime (GCCS-M) and Distributed Common Ground System Navy (DCGS-N) Increment II at the tactical edge at sea.

The Joint Regional Security Stack (JRSS) is a key JIE capability being delivered over FY16 and FY17 as part of the Single Security Architecture that will enable improved command and control of the DoD Information Network (DoDIN), improved cyber security and enhanced network operations. The Navy has shaped the evolution of JRSS to incorporate additional security capabilities that are currently being used in the Navy's security stacks today. We will transition to JRSS in FY18.

The Navy also fully supports the Director of National Intelligence and the Intelligence Community's (IC) effort to enable greater integration, information sharing, and security through an enterprise approach called the IC Information Technology Enterprise (IC ITE). Much as in the case of the UNCLASSIFIED- and SECRET-level JIE, the Top Secret/Special Compartmented Information (SCI)-level IC ITE is largely a shore-based infrastructure, and Navy's responsibility extends to the tactical edge at sea. IC ITE capabilities will be provided to all authorized Navy personnel afloat, ashore, and aloft by means of the following: (1) the Office of Naval Intelligence (ONI) SCI IT, Joint Deployable Intelligence Support Systems (JDISS), Global Command and Control System Integrated Imagery and Intelligence (GCCS-I3), and designated General Defense Intelligence Program (GDIP) elements ashore; and (2) the CANES

network, ADNS Increment III router, NMT transceiver, and such hosted and connected applications as the Ship's Signals Exploitation Equipment (SSEE) Increment F and DCGS-N Increment II at the tactical edge at sea.

Navy's transition planning for both JIE and IC ITE includes rationalizations of current data/applications, desktops, networks/domains, and cloud services to identify possible onramps to respective JIE and IC ITE services. That planning focuses heavily on the requirement to ensure such enterprise services – cloud-enabled and otherwise – operate with maximum effect around the clock at the tactical edge, in our case, at sea. As stated earlier, we will satisfy that fundamental requirement through our programmed modernization efforts that leverage not only CANES, ADNS Increment III, NMT, GCCS-M, DCGS-N Increment II, and SSEE Increment F but such other important Navy Programs of Record (PoR) as the Integrated Security Services Program (ISSP) and Tactical Switching (TsW). While so doing, we will be aggressive in leveraging any and all gains made by the JIE and IC ITE architects as they partner to set conditions for improved integration and interoperability across collaboration, identity management, information sharing, visualization, data access and other key touch points for national to tactical warfighting synergy.

Information-Age Warfare

The digital revolution has forever changed the very nature of warfare, and the cyber domain is now as important as getting underway, launching a Tomahawk or landing an aircraft – it is "Commander's Business." This change offers both challenges and opportunities. We now have non-kinetic warfare options that can be combined with kinetic options to fill-out the Warfighting Commander's quiver. Bits and bauds have the potential to disrupt adversary command and control nodes with similar effects to the 500-pound bombs we relied on in past conflicts and continue to rely on today. Our networks are now weapons systems and must be protected accordingly.

In response to the maturing nature of information-age warfare, six years ago, in 2009, we brought together the Oceanographic and Meteorological, Information Warfare, Information Professional, Intelligence, and Space Cadre officer communities – together with their enlisted, reserve, and civilian counterparts – to establish a professional and technically diverse warfighting corps on par with our surface, submarine, and aviation counterparts. The members of

this Information Dominance Corps are not the only Sailors executing Information Dominance as a warfare discipline, but they are its principal practitioners, and they bring extremely valuable skills and specialized knowledge to the fight. Moreover, they are taking on leadership roles at the highest levels, as exemplified most recently by Admiral Mike Rogers' confirmation as Commander, U.S. Cyber Command, and Director, National Security Agency/Central Security Service; as well as Vice Admiral Jan Tighe's command of Fleet Cyber Command/U.S. 10th Fleet.

Recent real world events and attacks on our networks and systems make clear that the cyber threat is increasing, Most of our networks were neither designed, procured nor maintained to be weapons systems or protected against sophisticated adversaries in this new warfare area. To address this issue, we continue to execute Task Force Cyber Awakening (TFCA), a year-long initiative established in August 2014 to (1) continue to track and oversee the execution of our defense-in-depth cyber approach in response to adversary activity on our networks, (2) gain a holistic view of cyber security risk across the Navy, (3) deliver fundamental change to the Navy's organization, resourcing, acquisition and readiness, and (4) align and strengthen authority and accountability in cyber security. We find ourselves in the position where we must modernize our older systems to mitigate vulnerabilities and limit the potential consequences that could disrupt our operations. At the same time, we must lay the foundation for the future, putting in place capabilities like Cyber Situational Awareness, which will give us the ability to monitor and detect cyber threats. We are also designing-in resiliency in current and new programs by generating common standards and protocols that will be used as guiding principles during procurement, configuration and implementation. Combined, these actions will improve our cyber posture, reduce the number of disparate systems in the Fleet, and increase the resiliency of those systems while providing the capabilities that the Battle Force of tomorrow will require.

Fight for Talent

I share the concerns of many of my colleagues in regards to the fight for talented people. Our business is becoming ever-more technical, complicating Navy's requirement to access, train and retain our Nation's best and brightest. Navy must compete not only against our sister services for this unique talent pool, but also against the corporate IT giants…whose pay and compensation packages can be more lucrative and workplace environments less severe.

Considering the exponential rate of change in technology and its corresponding impact on both our own and our adversaries' capabilities, the unique talents and abilities within the Information Dominance Corps are increasingly critical. With that in mind, we are in the process of reviewing and revising our Information Dominance Corps accession, training and education, and detailing processes so that we can recruit and retain the skilled and talented experts and leaders needed to meet the increasing demand signal from Warfighting Commanders and the Navy as a whole. We recognize that we must compete for that talent, and are looking to gain any possible advantage in that effort.

Conclusion

Warfare in the Information Age demands that the Navy, and our sister services must adapt and change. We in the Navy, through our recognition of this new warfare domain, our embrace of emerging technologies, our support for DoD and Intelligence Community modernization and efficiency efforts and, perhaps foremost, our creation of a dedicated Information Dominance Corps of information warriors demonstrate our resolve to excel in this area. We embrace our leadership role within the DoD on many of those fronts. We stand committed and ready to fight and win a potential conflict, on, above or below the sea, in space or in the information domain.

Thank you for your time and attention to these matters.

QUESTIONS SUBMITTED BY MEMBERS POST HEARING

FEBRUARY 25, 2015

QUESTIONS SUBMITTED BY MR. HUNTER

Mr. HUNTER. Has the Department considered revising the Cloud Computing Services deviation to allow for more flexibility for mission owners and cloud service providers in obtaining a Provisional Authorization (PA) for a dedicated or private cloud service while going through a contracting motion? As an example, a vendor may be awarded a contract, but PA is a contingent milestone of the contract award.

Mr. HALVORSEN. The DFARS Class Deviation on Contracting for Cloud Services currently requires that a commercial cloud service provider be granted a DOD Provisional Authorization (PA) prior to contract award. The Department is considering modifications to the policies and procedures currently specified in the Class Deviation, including whether a PA should continue to be a prerequisite for contract award, as part of its deliberations regarding DFARS Case 2013–D018. That DFARS case is planned to supersede the Class Deviation, and the Department will be seeking public comment on the new DFARS coverage through the public rulemaking process.

Mr. HUNTER. The DOD software inventory plan executed under section 937 of the FY National Defense Authorization Act included numerous exemptions, did not require an automated solution to compile the inventory, and it did not include an audit trail. These and other requirements are outlined in section 935 of the FY14 National Defense Authorization Act which your office is currently developing a plan to be submitted to Congress by the prescribed timeline of September 30, 2015. Please detail for the committee how your office is developing this plan, the input received from the services, and how your office is reaching out to industry to understand what automated capabilities exist and how this inventory can be performed to the satisfaction of both parties?

Mr. HALVORSEN. The FY14 NDAA Section 935 planning effort is ongoing. Efforts to date have been directed towards developing a business case analysis (BCA) of alternative courses of action for an enterprise software inventory reporting process. The BCA outlines several alternatives with varying degrees of centralized software license management and reporting operations to determine the most appropriate approach for DOD. As part of the BCA, the DOD Chief Information Officer (CIO) is analyzing two ongoing internal information technology (IT) management reporting efforts to determine the extent to which they could be leveraged to support the Section 935 software license reporting requirements. The DOD plan will build on these internal efforts to formulate a holistic approach for software license reporting. Once the appropriate software license reporting framework is selected, DOD CIO will develop a plan for a software license reporting process. The plan will be completed by the end of FY15

The DOD CIO issued a memorandum in June 2014 directing the CIOs of the Military Departments and DISA (the Components) to designate action officers to support DOD planning efforts for the Section 935 requirements. Through joint bi-weekly meetings hosted by DOD CIO, the Components' action officers have been collaborating in the planning efforts and reviewing work products. The Components have been an integral part in identifying the overall strengths, weaknesses, opportunities, and threats for each of the alternatives being considered in the BCA.

The joint team has reached out to industry by: 1) hosting commercial IT asset management (ITAM) and software license management vendors to present overviews and demonstrations of their product and service offerings; 2) meeting with corporate software license management teams to share lessons learned from their software asset management (SAM) implementations; and, 3) meeting with ITAM industry analysts to discuss DOD requirements and potential SAM implementation options. The DOD joint team has used industry benchmark data and lessons learned in support of its BCA alternatives. The DOD CIO and Component CIO representatives also meet with ITAM and other software providers through ongoing DOD Enterprise Software Initiative (DOD ESI) IT strategic sourcing operations. The DOD joint team has shared lessons learned about Component-level implementations of ITAM processes and tools using commercial software products. The Components have also independently reached out to industry to assess alternatives for Component-level ITAM and SAM efforts.

Mr. HUNTER. Please detail the Army's efforts to date on software inventory as prescribed by both section 935 of the FY13 National Defense Authorization Act and section 937 of the FY14 National Defense Authorization Act?

General FERRELL. The FY13 National Defense Authorization Act (NDAA), Section 937, required the Department of Defense (DOD) Chief Information Officer (CIO), in consultation with the CIOs of the Military Departments (MILDEP), to issue a plan for the inventory of selected software licenses, and to assess the need for the licenses. Under the auspices of the DOD CIO, all Services, Defense agencies and DOD Field Activities were directed to conduct an inventory of selected software licenses, including a comparison of software licenses purchased to licenses installed, and to submit a projection of the licenses needed over the following two years. The intent was to provide baseline information to enable economies of scale and cost savings in future procurement, use and optimization of the selected software licenses. Under the direction of the HQDA CIO/G–6, the Army assembled an integrated product team (IPT), with representation from all Army organizations and the Joint Commands for which Army is the executive agent, to conduct a selected software license inventory (SSLI). Meeting on a weekly basis, first with key stakeholders to develop the plan, and then with all appropriate organizations, the IPT provided oversight for conducting the SSLI audit. The audit used automated scanning and discovery tools where available, and a data call for networks or enclaves where automated tools were not readily available. CIO/G–6 aggregated and rationalized the inventory reports and completed the analysis of selected software licenses purchased in comparison to software licenses installed. The SSLI effort included a projection of future need for these licenses over the following two-year period. The initial report was submitted to the DOD CIO on July 18, 2014; after providing some additional information and clarifications, the final report was submitted on August 28, 2014. The Army owned 250 of the 937 titles included in the selected software list. We estimate that the SSLI audit across the Army involved approximately 400 personnel and 10,000 hours over an eight-month period. FY14 NDAA Section 935 directed DOD to update the plan for the inventory of selected software licenses, to include: inventorying all software licenses utilized within DOD for which a military department spends more than $5 million annually on any individual title; a comparison of licenses purchased to licenses in use; and plans for implementing an automated solution capable of reporting software license compliance with a verified audit trail and verification by an independent third party. It also mandated the plan provide details of the process and business systems necessary to regularly perform reviews, and a procedure for validating and reporting the registration and deregistration of new software. The updated plan is due no later than September 30, 2015. In support of the FY14 NDAA, CIO/G–6 established a pilot project to test commercial software asset management (SAM) tools that will, ultimately, provide the Army the capability to manage software licenses across the enterprise. The SAM pilot is intended to test feasibility and scalability across Army networks, as well as commercial best practices and business processes for managing software utilization, entitlements and license compliance. Additionally, the Army CIO/G–6 continues to support the DOD CIO's Software License Management Tiger Team effort. This team is updating the plan developed per FY13 NDAA Section 937 and is on track to meet the 30 September deadline. The DOD effort has included a working group to determine potential solutions to satisfy DOD reporting requirements and a follow-on effort to determine the most practical and cost-effective solution for the DOD enterprise.

Mr. HUNTER. Please detail the Army's efforts to date on software inventory as prescribed by both section 935 of the FY13 National Defense Authorization Act and section 937 of the FY14 National Defense Authorization Act?

General BENDER. In 2013 the Air Force initiated network scans to determine the amount of DOD/CIO-selected software installed on Air Force-managed sections of the NIPR and SIPR networks. The Air Force is also presently performing research and analysis of existing data repository tools as an interim solution to consolidate, manage, and report current software inventory. Another interim solution is the leveraging of existing scanning tools such as Microsoft's Host-based Security System (HBSS) and Systems Center Configuration Manager (SCCM) to collect and analyze installed software applications until a permanent automated software license management solution is determined. In early and proactive efforts to identify a license management solution, the Air Force released a Request for Information (RFI) to industry requesting the identification of software solutions capable of addressing the Air Force's Information Technology Asset Management (ITAM) requirements. Solutions from 46 small and large businesses included the use of commercially available software with implementation options including leveraging current government personnel and processes, primarily contractor support, and some level of hybrid approach. These options are presently under consideration, however, discussions with

DOD/CIO and other military departments (MILDEP) have identified that there is not a singular solution to resolve the software license management task at hand. Regarding the DOD/CIO and other MILDEPs; the Air Force has actively participated in discussions and working groups in efforts to identify present software license management processes and tools as well as a joint solution. The Air Force has also been an active participant in the interagency agreement supporting the DOD Joint Enterprise License Agreement (JELA) effort and will continue to leverage the JELA process to determine software needs for the next two years.

The Air Force will continue to aggressively identify, collect, and report software licenses in accordance with license agreements and congressional directives. Efforts and preparations are ongoing to meet both Section 937 of the National Defense Authorization Act (NDAA) for 2013 and Section 935 of the NDAA for 2014 as well as that of Section 1003 of the NDAA for 2010, Financial Improvement and Audit Readiness (FIAR). The Air Force is working toward a viable solution to not only meet the intent of the two NDAAs but to also establish an equitable solution for the future management of its entire ITAM program.

Mr. HUNTER. Dr. Zangardi, please detail the Navy's efforts to date on software inventory as prescribed by both section 935 of the FY13 National Defense Authorization Act and section 937 of the FY14 National Defense Authorization Act.

Dr. ZANGARDI. The Department of the Navy (DON) is actively engaged in the Department of Defense Chief Information Officer (DOD CIO) Integrated Product Team (IPT) for Information Technology Asset Management (ITAM) created to address reporting requirements prescribed by Section 937 of the FY13 National Defense Authorization Act (NDAA) and revised by Section 935 of the FY14 NDAA. The DON used available IT portfolio management tools and authoritative data sources to prepare the DON software license inventory and needs assessment submitted to the DOD CIO and will continue its support of the DOD CIO Joint IPT as it works to comply with the requirements of the Acts.

Mr. HUNTER. Please detail the USMC's efforts to date on software inventory as prescribed by both section 935 of the FY13 National Defense Authorization Act and section 937 of the FY14 National Defense Authorization Act?

General NALLY. The Marine Corps, in coordination with the Department of Defense (DOD), completed an inventory of all software that met the established criteria per Section 937 of National Defense Authorization Act (NDAA) 2013. The Marine Corps inventory has been submitted in accordance with the July 18, 2013 DOD Chief Information Officer memorandum, Subject: Department of Defense-wide Selected Software Licenses Inventory Plan.

Marine Corps representatives are ongoing participants in the software license planning meetings established by the DOD Chief Information Officer in the May 30, 2014 memorandum, Subject: Establishing a Joint Software License Reporting Team for the Fiscal Year 2014 National Defense Authorization Act. The Marine Corps provides input for requirements and supports development of the DOD plan.

The Marine Corps is developing an Information Technology Asset Management Module (ITAMM) and License Management Module (LMM) within its BMC Remedy environment to replace the legacy Virtual Procurement Management System (VPMS) customer software ordering tool. With the sun-setting of VPMS in FY16, ITAMM and LMM will enable the Marine Corps to identify what software is purchased and in conjunction with approved network software discovery tools, track what software is in use on the Marine Corps Enterprise Network (MCEN) in order to identify discrepancies for remediation.

All requests to procure software products are processed through the Marine Corps Information Technology Procurement Review and Approval System (ITPRAS) and require registration in the DON Application and Database Management repository prior to final approval by Marine Corps Director C4/Deputy DON Chief Information Officer (CIO) (Marine Corps). Software is captured in the appropriate functional area portfolio and Functional Area Managers retain responsibility to regularly perform reviews of and validate and report on their portfolios to the Director C4/DDCIO–MC. The Marine Corps continues to work with the DOD and DON CIO Integrated Product Team (IPT) for Information Technology Asset Management (ITAM) created to address reporting requirements prescribed by Section 937 of the FY13 NDAA and revised by Section 935 of the FY14 NDAA.

○