



DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

DEFENSE
INFORMATION
SYSTEMS
AGENCY

STRATEGIC PLAN 2015 – 2020



UNITED IN SERVICE TO OUR NATION





DIRECTOR'S STATEMENT

We are at an operational crossroads. We continue to operate in a contested battlespace, where the barrier to entry is low and oftentimes unchallenged. We must recognize that mission success is defined by our ability to pre-emptively disrupt, degrade, or deny our adversaries, both internal and external, unimpeded access to the information and capabilities of the Department of Defense Information Network (DODIN). We must sustain our operations and defenses before, during, and after an attack by reducing the attack surface, continually improving defensive cyberspace operations, and effectively commanding and controlling the DODIN.

We are the premier Information Technology Combat Support Agency that provides and assures command, control, communications, computing, intelligence, surveillance, and reconnaissance (C4ISR) to the warfighter. We deliver enterprise services and data at the user point of need. We now serve as the joint operational arm of defensive cyberspace operations, for the Department of Defense.

Our Mission requires that we remain purposeful in planning, acquisition, operations, and execution. As the provider for defensive cyberspace and IT combat support for the DoD we will:

- **Focus on our global infrastructure of telecommunications and services delivery — comprised of a hybrid cyberspace ecosystem of mobile, collaboration, internal clouds, and commercial clouds.**
- **Synchronize command and control (C2) and senior leadership support to effectively streamline decision making within all echelons of National and DoD leadership.**
- **Enable warfighter capabilities from a sovereign cyberspace domain, focused on speed, agility, and access.**
- **Reduce costs by eliminating duplication in production and operations.**

We will be aggressive in our pursuit of efficiency and effectiveness, and no longer support the operations of legacy and costly applications without senior leadership's approval and direction. We recognize our value added within this mission space and will continually fine tune our efforts. This Agency will remain in step with, or ahead of, our mission partners and proactively evolve capability requirements to meet operational needs.

We will bring the business of defensive cyberspace operations support for the DoD under one roof – Our Roof.

The Joint Information Environment (JIE) remains the cornerstone of the Department's future – providing a secure information framework from which our national senior leaders and joint force commanders, command and control forces that deliver responsive, decisive actions from any device; anytime anywhere.

We will continue to lead the DoD cyberspace and information technology optimization efforts. This includes eliminating Department duplication of effort, capitalizing on the range of commercial cloud solutions, and maintaining the operational cyberspace integrity of the DODIN services we defend, operate, and assure. Our agile enterprise will emphasize on-demand, real-time, 24x7, secure access and availability.

Over the next several months, DISA will:

- Evolve the Joint Force Headquarters – DODIN (JFHQ-DODIN)
- Deploy and operationalize the Joint Regional Security Stacks (JRSS) platform
- Continue to implement our reorganization
- Maintain our superior delivery of capability to our mission partners
- Enhance mobility and collaboration capabilities

This message sets out an action-based plan for the future. Our future state will include common enterprise services and single-user interfaces with multi-level security and normalized data. Cyberspace workforce development will continue to evolve through cooperative efforts with our Intelligence Community (IC) and industry partners to enable a multi-faceted, highly skilled countermeasure to nation states, rogue entities, insider threats, and malicious attacks by hackers. We will manage risk within the execution of our cybersecurity mission through standardization, reciprocity, and continuous monitoring to achieve information dominance.

We are a professional and innovative civilian and military team. Along with our mission and industry partners, we will continue to produce valued results. DISA is adapting to the changing cyberspace, technological, and fiscal environments. We will ensure that we monitor our progress through meaningful and measurable metrics and analytics that will be exposed for internal consumption by the workforce.

We are first and foremost The Department of Defense's Defensive Cyberspace IT Combat Support Agency.

We cannot allow ourselves to be held to an era or standards that point to the past and the way “things used to be.” We must always look toward the horizon, the next conflict, the next opportunity to answer the call and assist in Defending the Nation and her sovereign interests.

**We are DISA –
United in Service to Our Nation!**

Ronnie D. Hawkins, Jr.
RONNIE D. HAWKINS, JR.
Lieutenant General, USAF
Director



THE DISA VISION

Information superiority in defense of our Nation.

THE DISA MISSION

DISA, a Combat Support Agency, provides, operates, and assures command and control, information-sharing capabilities, and a globally accessible enterprise information infrastructure in direct support to joint warfighters, national-level leaders, and other mission and coalition partners across the full spectrum of operations.

THE OBJECTIVE STATE

Assured, scalable, managed access to services and data
In all environments
At the point of need
Provided from cost-effective infrastructure and computing.

We are increasing our investments in cyber, in recognition of the growing threat that cyber poses to our national security and critical infrastructure. — Ashton B. Carter, Secretary of Defense



OUR PLANNING METHODOLOGY

DISA's planning methodology consists of the development of two plans: the Strategic Plan and the Strategic Roadmap. The DISA Strategic Plan is influenced by overarching Department-level guidance and provides a common understanding of our Agency mission and vision, and further identifies the strategic goals and objective state that prioritize our efforts and postures the Agency for the future. Included in the plan is a technology outlook that drives technology investments for the Agency.

The Strategic Plan guides the development of a Strategic Roadmap which identifies objectives, major actions and tasks, and resource alignment to meet our goals. These plans form our framework that supports the Department's vision to achieve a more effective, secure, and efficient enterprise for the DoD and the Nation. The target delivery of the Strategic Roadmap is October 2015.



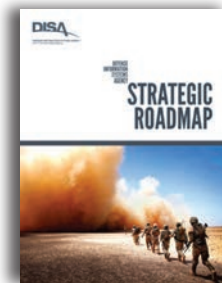
DEPARTMENT-LEVEL GUIDANCE



PERFORMANCE METRICS & REPORTING



STRATEGIC PLAN



STRATEGIC ROADMAP



The military that maintains the most agile and resilient networks will be the most effective in future war. This is the kind of force we are building for the future. – General Martin E. Dempsey, Chairman, Joint Chiefs of Staff

OPERATING PRINCIPLES

DISA's operating principles provide the tenets by which the Agency makes key strategic decisions. These principles guide our actions.

Single Point of Entry

The need for one entry point to access DISA information and services to:

- Enhance Customer Relationship Management (CRM) processes focused on automating, to the maximum extent possible, the requirements management and fulfillment components of our services
- Enhance DISA's outreach efforts enabling DISA personnel to accurately and concisely promote current and planned DISA services, and improve responsiveness to mission partners' emerging requirements (e.g. Integrated Priority Lists (IPLs), COCOM Campaign Plans)

Optimize Department Investment

Enable the Department to maximize use of its resources by providing cost-efficient capabilities; an effective and defensible infrastructure; and standardized support services, business processes, and policies that enable the rapid infusion of technology into the enterprise

- Streamline Agency acquisition and contracting processes to support the enterprise
- Manage mission partner requirements to achieve strategic sourcing cost and performance efficiencies, eliminate duplication and maximize Enterprise License Agreements (ELAs)

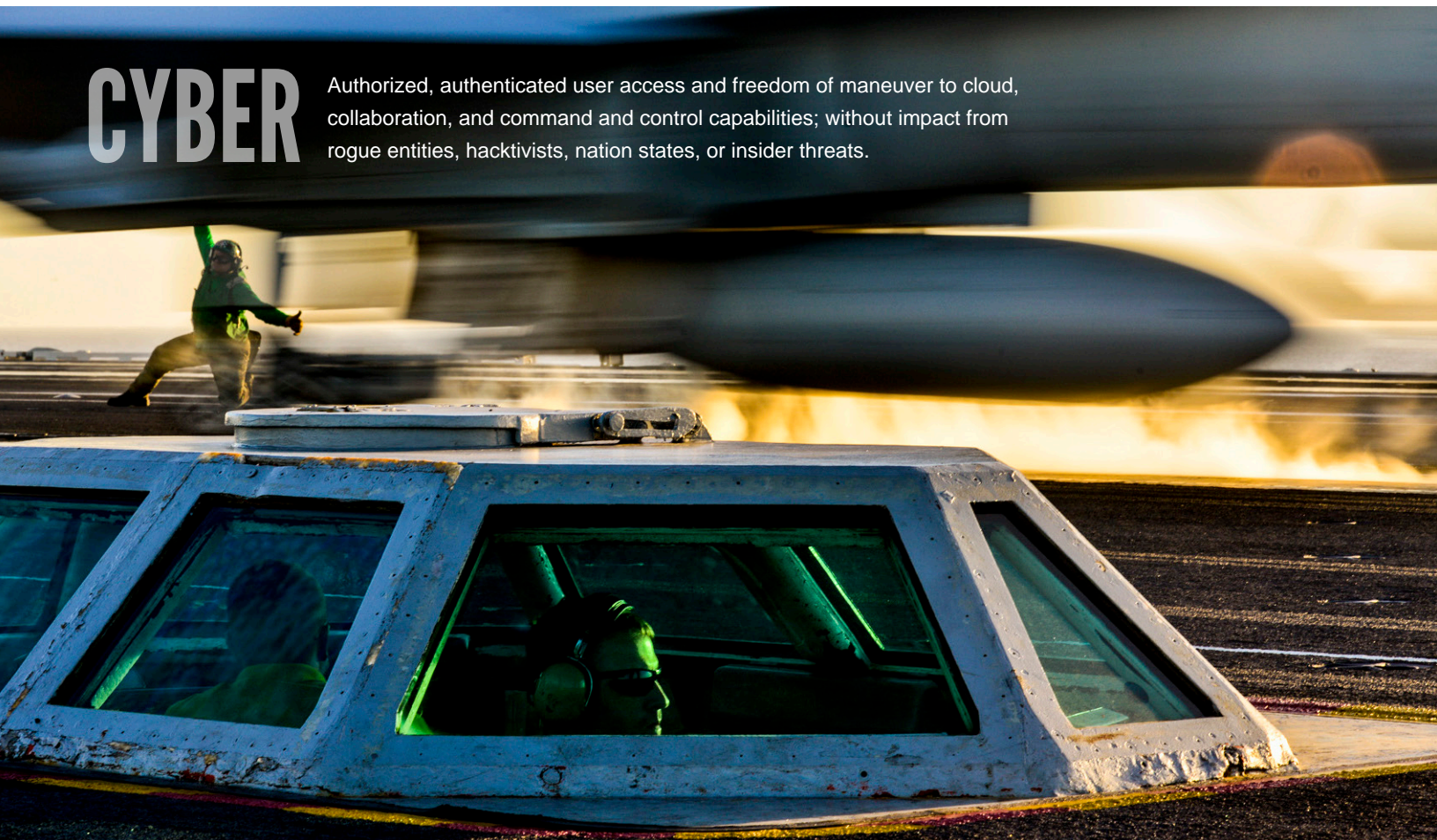
Agility & Speed to Market

Implementation of acquisition and procurement best practices that allow for agility in development, and rapid deployment of capabilities to the warfighter

- Continue the DISA-first fielding and test methodology
- Enable our mission partners to rapidly innovate independent of DISA by leveraging DISA and commercial services

CYBER

Authorized, authenticated user access and freedom of maneuver to cloud, collaboration, and command and control capabilities; without impact from rogue entities, hackers, nation states, or insider threats.



THE DISA STRATEGIC GOALS

Provide Global Infrastructure

We will develop, test, deploy, sustain, and maintain a global elastic infrastructure, spectrum, computing, and storage capabilities that will support full spectrum collaboration. The foundational elements of those services will be comprised of reusable components. All elements will be normalized, converged, and available at reduced cost, increased usability, and maximum portability to mobile platforms. We will expand our delivery of enterprise services to the Services, agencies, and DoD and national-level leadership.

Provide Mission Partner and Leadership Support

We will design, develop, implement, and maintain optimized, cost-efficient, interoperable decision support systems to be used by mission partners at all levels of senior leadership. We will ensure senior leadership has a modernized, reliable suite of services and capabilities that enhance the execution of crisis management, coalition, and deliberate planning activities.

Provide Command and Control (C2) and Enable Cyberspace Sovereignty

We will execute synchronized DODIN command, operations, and cyber defense missions to ensure freedom of maneuver for the warfighter and mission partners. We will establish, train, and implement cyber workforce elements; shape readiness through continuity programs; and execute synchronized operations that will offer us more visibility and response to cyber threats.



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.

– Terry Halvorsen, *DoD CIO*



CLOUD

Scalable user access at the point of need for software, processing, and infrastructure and storage services.

CHIEF TECHNOLOGY OFFICER'S TECHNOLOGY OUTLOOK



The need for information superiority has never been greater — across the spectrum of military operations and within a contested battlespace which includes the cyber domain.



Mobile devices and applications, as well as cloud computing services continue to transform our operational landscape and enable greater mission effectiveness through improved communication, access, information sharing, data analytics — resulting in more rapid operational response times. Research in the areas of communications, networking, cybersecurity, and enterprise services continue to produce capabilities that significantly enhance our warfighting and business systems and services.



Ensuring the viability of technological solutions that meet current and future requirements of the Department's information environment requires that we efficiently integrate mature solutions, and at the same time influence research and technology initiatives that address our most critical gaps and capability shortfalls. DISA's technical strategies ensure these emerging capabilities are well-engineered and provide technically sound solutions. These strategies are the basis for the development, integration, and operations of the Agency's critical cyber-based capabilities and services.



TOMORROW AND BEYOND

The growing information demands of our users necessitate that DISA excel in the identification and characterization of technological advancements that hold future relevance and benefit to the Department. DISA will continue to maintain the DISA Technology Watchlist — a set of key technology areas that are the most critical for DISA to understand, acquire, and evolve over the next 5 years. DISA will effectively manage the identification, acquisition, adoption, insertion, and integration of advanced technology into DISA systems and operations. DISA will also employ robust techniques of technology assessment and characterization, experimentation, and piloting. The ability to conduct quantitative and qualitative technology evaluations, experiments, proof of concepts, and piloting activities is critical to the successful integration of these technologies and capabilities. The DISA Technology Watchlist identifies specific technology areas that contribute to the future of the following capabilities:



- **Networking technologies** that will improve the performance, reliability, adaptability, and security of DoD networks and collapse today's multiple encrypted network enclaves (NIPRNET, SIPRNET, Coalition, etc.) into a single, integrated transport network.
- **Computing and storage technologies** that will transform today's fixed, redundant computing and storage solutions to an elastic data environment where compute and storage capacity is flexible, interoperable, and transient.
- **Unified Capability technologies** that will improve productivity, strengthen information sharing, and enhance the teamwork of DoD warfighters and civilian personnel.
- **Mobility Device and Application technologies** that will evolve the DoD enterprise to where all personnel have the freedom of action to securely work in any location, over any device, across any network.
- **Cybersecurity technologies** that will strengthen the resiliency of defense-in-depth cybersecurity posture to absorb major attacks without any significant disruption to DoD operations.
- **Network Operations technologies** that will ensure the continuity of cyber domain operations in the face of disruption and attack, adversary activity is known, and cyber threats are mitigated.



CYBERSPACE supports operations extensively in all of my mission areas and has become a critical facet of national power. We must continue to develop a robust cyber mission force with the authorities, skills, and resources to protect against a maturing set of cyber threats.

– Admiral Cecil D. Haney
Commander USSTRATCOM



COLLABORATION

Warfighters, coalition, intergovernmental organizations and industry with access to mission partner and enterprise-wide capabilities.



COMMAND & CONTROL OF THE DODIN

Cyber workforce and mission assurance professionals executing operational control of the DODIN infrastructure and computing resources.

The current **CYBER THREAT** environment is uncertain and ever changing. What is certain, however, is the pervasive nature of those cyber threats and the increasing sophistication of adversaries.

– Admiral Michael S. Rogers
Commander USCYBERCOM



The DISA Chief Technology Officer (CTO) is responsible for the development of the overall technical strategies, technical review, and technical oversight of the Agency's products and services. The CTO's objective is to assist in making relevant and well-informed technology investment decisions for DISA. We achieve these outcomes by conducting technical reconnaissance, assessing critical and promising technology solutions, and developing technology forecasts and innovation roadmaps for existing and future DISA programs. DISA continues to expand technology outreach activities by establishing relationships with key stakeholders in DoD, Government, industry, and academia. The partnerships are critical to forecasting and focusing promising technologies for innovative enterprise solutions and an enhanced information environment.

CONCLUSION

As the IT Combat Support Agency for the Department of Defense, we are committed to our mission partners.

We commit to:

- **Acquiring, integrating, delivering, operating, and sustaining the best services and capabilities in cyber, cloud, collaboration, and command and control**
- **Providing a robust, synchronized, normalized, and mobile accessible infrastructure and computing environment**
- **Enabling the seamless immediate connection, sharing, and assured access to the full suite of information capabilities and enterprise services**

This plan describes DISA's fundamental goals that form the core of our commitment — our high-level strategy to deliver global infrastructure, mission partner and senior leader support, and enable cyberspace sovereignty for the warfighter.

Our people are our strength. That ethos, coupled with our leadership's desire to meet the Department's fiscally challenged and resource-constrained operational environment head-on, will drive us to identify efficiencies, eliminate duplication, and channel our resources into the highest priorities.

We will balance our execution constraints and the growing need to adopt technologies that enable the freedom of maneuver in the cyber domain.

We will continue to align resources and shape our workforce to meet the needs of the Department and our mission partners.

Rest assured, we don't take the commitment to our mission partners lightly. We are a key enabler for their success and we are in this together.

WE ARE DISA.



We are global professionals vital to the defense of our Nation

We respond to mission priorities with speed and urgency

We embrace the values and potential of our people

We engage through a collaborative environment

We know diversity leads to innovation

We believe individual growth, learning, and proficiency are critical to our future

We value perseverance and recognize failure as a growth opportunity

We build trust through transparency

We hold ourselves accountable

We are United in Service

WE ARE DISA

DEDICATION

INTEGRITY

SERVICE

ALWAYS



DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

DISA STRATEGIC PLAN 2015-2020
06.10.2015