STRATEGIC VISION 2012-2017

One Mission · One Team · One Agency

Grant Schneider, Deputy Director for Information Management and Chief Information Officer

DS • DIRECTORATE FOR INFORMATION MANAGEMENT AND CHIEF INFORMATION OFFICER

COMMITTED TO EXCELLENCE IN DEFENSE OF THE NATION

Table of Contents

400

DEFENSE INTELLIGENCE AGENCY

DS • DIRECTORATE FOR INFORMATION MANAGEMENT AND CHIEF INFORMATION OFFICER

The Directorate for Information Management and Chief Information Office (DS) and its mission are critical to our nation's security. Information Technology (IT) is a vital asset to intelligence analysts, warfighters, and national policy makers as they execute their mission. Threats to IT systems and information security are evolving; DS' technology must evolve accordingly. We must defend against changing and diverse threats while delivering reliable and consistent services to our customers ensuring the success of the Department of Defense Intelligence Information System (DoDIIS).

The realities of today's fiscal environment determine how DS will meet our mission and respond to the strategic imperatives before us. Driven by our customers' priorities, our focus is on enhancing the nation's technology advantage and on providing an environment for secure, collaborative information sharing.

Our customers rely on us to deliver on our commitments because we execute the U.S. national security mission through IT capabilities. President Obama reiterated the importance of IT to national security when he said:

> *"Our technological advantage is a key to America's military dominance…From now on, our digital infrastructure —the networks and computers we depend on every day—will be treated as they should be: as a strategic national asset…We will ensure that these networks are secure, trustworthy and resilient."* [1]

DS is strengthening commitment to our customers through security and collaboration. Additionally, we are providing products and services that deliver mission advantage resulting in greater trust across Defense Intelligence Agency (DIA) and DoDIIS. The DS Strategic Vision will attain this and will guide DS' priorities, plans, resource allocations, and actions from fiscal year 2012 to 2017. Three change imperatives guide the DS strategy:

1. Enhance our technology advantage.
2. Build customer trust to strengthen DS as the preferred IT provider for DIA and DoDIIS.
3. Achieve operational excellence.

The DS Strategic Vision reflects these imperatives and describes four actionable, measurable goals that lead to outcomes addressing our customers' concerns:

Goal 1: Facilitate and Enhance Information Sharing across DoDIIS

Goal 2: Achieve World-class IT Security and Collaboration across Multiple Networks

Goal 3: Develop the DS Workforce

Goal 4: Operate Effectively and Efficiently

Ultimately, DS will establish One Secure Environment (OSE) that hosts multiple levels of classified information. DS also will be able to define and designate defense intelligence IT as a weapons system. Designating defense intelligence IT in this category ensures that IT receives the management attention, resources, and oversight necessary to meet warfighters' and policymakers' evolving technology needs.

I thank you for your commitment to DS' mission and your service to our nation.

Grant Schneider
Deputy Director of
Information Management and Chief Information Officer
of the Defense Intelligence Agency

Our Mission

DS delivers secure digital intelligence through IT supremacy, ensuring vigilant awareness, and enabling decision advantage anywhere at any time.

Our Vision

One agile, secure, global IT enterprise, driving information dominance throughout the operational spectrum in defense of our nation, by leveraging technology across all classification domains through OSE.

Our Role

DS must succeed for the nation's intelligence enterprise to succeed. Intelligence and information today are inherently digital; the nation trusts us to securely distribute that information so those involved in defense—from top decision makers to individual warriors—can secure our country. To fulfill this trust, we partner with those who contribute to the intelligence mission.

Introduction

IT plays a vital role in enabling the defense intelligence mission. An incredible challenge facing our nation is securing information from internal and external threats while enabling beneficial collaboration within our internal national security infrastructure. Specifically, DIA Director Lieutenant General Ronald L. Burgess, Jr. stated that DIA must stay ahead of the advanced pace of available information technology capabilities to timely address the challenges that face the defense intelligence mission. The DIA Strategy cites that "DIA must rapidly implement new and innovative approaches in order to outpace the application of low technology advantages by our nation's adversaries."[2]

The entire Defense Intelligence Enterprise (DIE), defined as the collection of the Department of Defense intelligence, counterintelligence and security communities,[3] is evolving its practices and developing new capabilities to support information sharing while being fiscally responsible. This will enable DIE to continue to fulfill its mission to "support our national, defense and international partners with "knowledge rich" all-source defense intelligence, counterintelligence, and security."[4] DoDIIS is a significant partner in the DIE community.

DS, through its leadership of DoDIIS, has a unique role in advancing the technical capabilities of DoDIIS as the architect and maintainer for all-source defense intelligence networks.[5] DS is leading the DoDIIS community into an era of new capabilities and enhanced delivery of intelligence information.

Five enduring principles, based on mission requirements, guide DS' actions to fulfill our mission as the technology provider for defense intelligence.

Guiding Principles

1. The customer mission is our mission. We partner with our customers to achieve their missions.

DS is a mission partner that aligns to customers' agendas and builds trust by providing solutions to help realize customer goals. Mission partnership requires a foundation of trust between DS and its customers. Trust starts with delivering consistent, reliable products and excellent customer service. Mission partnership goes beyond delivery to engaging with customers in early discussions to identify and solve customers' unique technology needs. DS, as the primary IT provider for DoDIIS, also collaborates closely with other organizations to shape IT solutions that advance missions in a timely manner. DS builds trust as a mission partner by consistently delivering on customers' requirements.

2. We enhance intelligence collaboration and communication across the Federal Government.

Effective intelligence production and use requires collaboration and communication. Intelligence analysts must connect with each other to link data that, in the aggregate, provides insight and context.[6] Designated warfighters, defense planners, national security policy makers, and international partners then receive intelligence information.[7] Developing and communicating intelligence requires consistent IT services enabled by DS. Equally significant, DS promotes a collaborative culture across DoDIIS and its mission partners, recognizing that collaboration and communication are behavioral and cultural practices that IT enables.[8]

3. We ensure IT security across the Defense and Intelligence Communities.

Threats to IT systems and information security are evolving and DS' technology must evolve accordingly. DS approaches IT security holistically to address complex, changing, multifaceted threats. We also provide secure common solutions across classified networks in order to protect our data without sacrificing access to tools or hindering connections among Intelligence Community partners.

4. We sustain technological advantage and agility within DIA.

DIA supports warfighters by providing intelligence information that influences tactical movements and strategic operations against U.S. enemies. As an agency DIA will be more agile, adaptable, and flexible so warfighters can use DIA products to adjust quickly to evolving threats in today's operational environment. Production and delivery of this intelligence is dependent on the technology that DS provides. DS is committed to agility by creating a secure IT environment that enables increased real-time information sharing, eases collaboration and analysis, and effectively distributes timely intelligence information to those who need it quickly. DS' efforts yield more accurate and time-relevant intelligence information and help our armed forces be more responsive to threats. DS is constantly striving to strengthen DIA's technological advantage today, and ensure that DIA retains its advantage in the future. We will remain ahead of the curve.

5. We demonstrate operational excellence as stewards of our citizens' precious resources.

The DS mission is ever-changing and essential to the defense of our nation, regardless of resource constraints. Budget realities dictate that

the defense intelligence community execute its mission with operational excellence, defined as the joining of effective execution and efficient resource use. DS strives to reduce redundancies and increase efficiency across the community. DS wisely uses its people, assets, and technology to effectively deliver relevant timely products and services, achieving more with fewer resources.

Change Imperatives

The Guiding Principles define broad, enduring, aims that guide DS as it fulfills its mission. The Change Imperatives are derived from the Guiding Principles and drive DS' strategic goals. Recent events as outlined below illustrate even further the necessity for change.

- In 2010, an Army soldier allegedly leaked classified information to the organization Wikileaks, which then used IT tools to release thousands of classified military and diplomatic documents through the web. The information compromise and the global disclosure of sensitive information potentially endangers U.S. troops and damages U.S. diplomatic relationships.
- In 2009, the Department of State listed Umar Farouk Abdulmutallab, the Christmas Day bomber, on a register of individuals with alleged terrorist connections; his name was not shared with American allies nor placed on the no-fly list, allowing the individual to board a transcontinental airliner with explosives.[9]
- China has allegedly launched numerous, varied, cyber attacks against the U.S. government, allies, and private industry partners since 2002 and will likely continue to attack our IT systems.[10]

The seriousness of the events above require direct action and the Change Imperatives reflect the breadth and depth of the response DS must take.

1. Enhance our technology advantage.

Events on the battlefield develop rapidly; warfighters and national security leaders need accurate, real-time, intelligence information. DS must maintain the technological advantage that helps DIA produce all source intelligence analysis. In the immediate future maintaining this technological advantage involves a multifaceted approach based on expressed customer needs. DS will provide reliable desktop services to help analysts across defense intelligence organizations and geographic locations fulfill their missions quickly. DS will evolve an IT infrastructure to facilitate information sharing and gain operational efficiencies. These actions meet the technology needs of individuals and the enterprise, while also meeting DS' need for cost-effective solutions.

2. Build customer trust to strengthen DS as the preferred IT provider in DoDIIS.

Establishing a reputation as the preferred IT provider is necessary for DS to become a trusted mission partner that customers turn to for effective day-to-day technology solutions and for solving unique, critical, mission needs. To become the preferred IT provider, DS will build trust by consistently delivering reliable IT products and services that enhance customers' IT experience. DS will also engage in early discussions with customers to drive mission solutions. These actions strengthen DS' relationship with individual customers and improve our standing as the preferred IT provider throughout DoDIIS.

3. Achieve operational excellence.

DS' mission is critical, constantly evolving, and ongoing. However, DS' resources are finite and may face reductions in the near future. By 2015, DoD plans to reduce IT costs as it encourages building centralized IT infrastructures, processes, and applications usable throughout defense agencies. DoD will also reduce the budget of the national intelligence apparatus as it looks to minimize unnecessary duplication. Regardless of budget cuts, our mission is vital and must be fulfilled. DS will adapt to budget reductions by transforming its organization, processes, and human capital to be more operationally efficient while providing customers with high quality products and services. We will execute our mission with operational excellence.

The Guiding Principles and Change Imperatives outline the drivers behind DS' Strategic Vision. Based on these drivers, DS has set the following goals that it will accomplish during the years of 2012 to 2017.

Goal 1: Facilitate and Enhance Information Sharing across the Department of Defense Intelligence Information System (DoDIIS)

Goal 2: Achieve World-class IT Security and Collaboration across Multiple Networks

Goal 3: Develop the DS Workforce

Goal 4: Operate Effectively and Efficiently

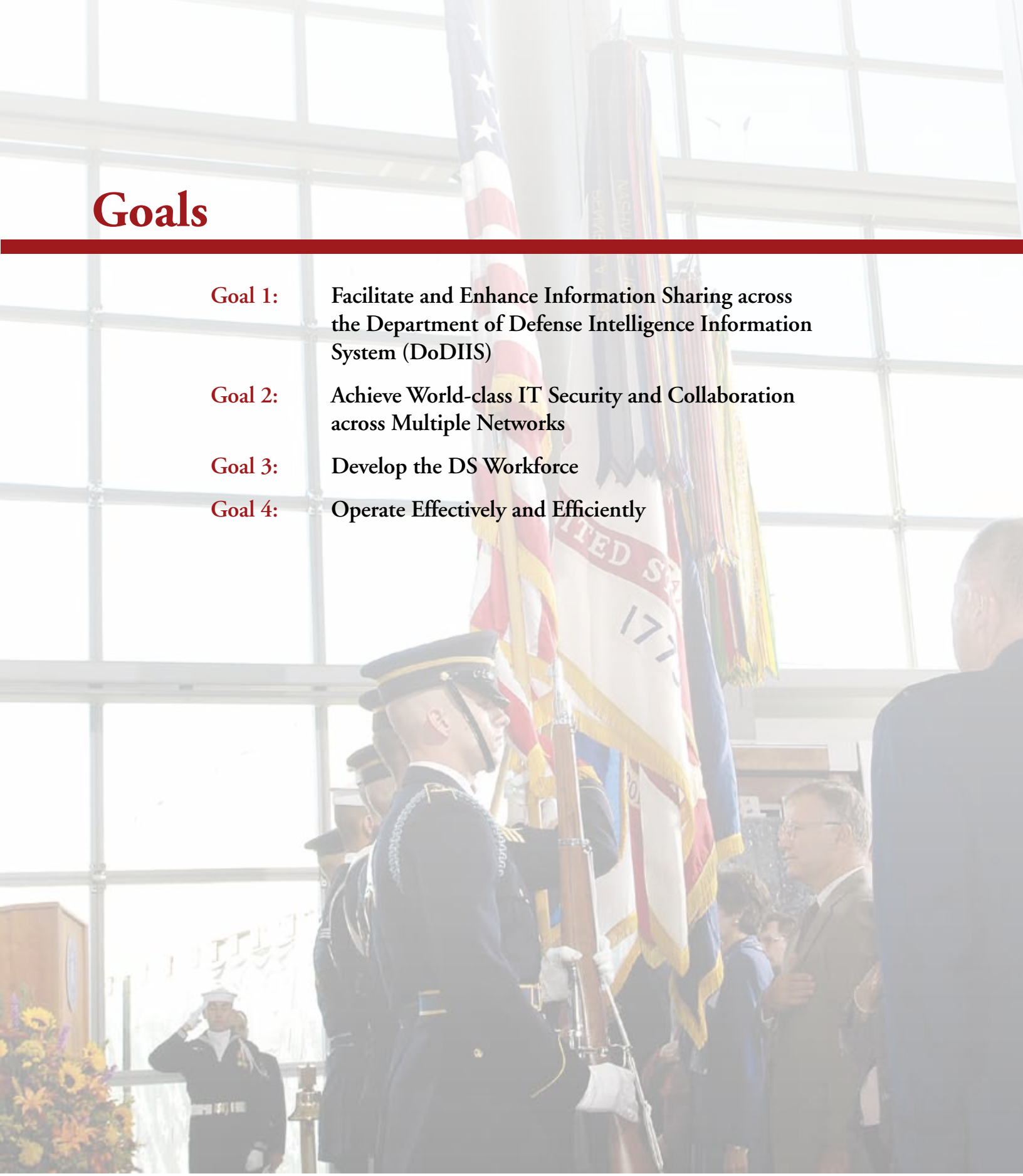
Ultimately, these goals will set the organizational and technical conditions for DS to achieve its vision after 2017.

During 2012 to 2017, DS will solidify operational efficiencies, trust, and credibility to perform as a mission partner that resolves customers' IT challenges. After 2017, DS will establish the OSE that hosts multiple levels of classified information. The OSE, based on the Private Cloud Network (PCN) instituted in the 2012-2017 period, will allow quicker and easier secure information sharing across agencies and classification levels.

DS' enhanced reputation and capabilities will enable the organization to define and designate defense intelligence IT as a weapons system. Defense intelligence IT will receive management attention, resources, and oversight necessary to serve warfighters' and policymakers' evolving needs and further DS' mission to defend the nation.

Goals

Goal 1:	Facilitate and Enhance Information Sharing across the Department of Defense Intelligence Information System (DoDIIS)
Goal 2:	Achieve World-class IT Security and Collaboration across Multiple Networks
Goal 3:	Develop the DS Workforce
Goal 4:	Operate Effectively and Efficiently



Goal 1: Facilitate and Enhance Information Sharing across the Department of Defense Intelligence Information System (DoDIIS)

The defense intelligence community understands information sharing is critical to advance the mission, facilitate effective and efficient war-fighting, conduct intelligence and business processes, and execute other national security activities. Over time organizational processes and technical silos have limited sharing and collaboration. Many agencies have unique technology infrastructures, making it difficult to exchange and synthesize valuable information across agencies.

DS is committed to building a network environment that enables simpler, timely, secure information sharing across DoDIIS, to allow more collaborative discovery, synthesis, and delivery of intelligence information between warfighters, defense planners, policy makers, and international partners.[11] Recognizing information sharing is predicated on skillful management of the risk of unauthorized disclosures, DS will enable information sharing while maintaining the highest levels of security.[12] Expanding information sharing at the IC level will be the first step to facilitating information sharing throughout DoDIIS. Policy and culture also play a role in advancing information sharing and DS will actively influence necessary policy guidelines and encourage an information sharing culture.

1.1: Enhance the cloud computing environment.

DS is continuously maintaining and improving DoDIIS global IT infrastructure to make information sharing easier. Budget realities dictate that DoDIIS IT infrastructure transforms to meet those needs efficiently and effectively as the DoD looks to reduce IT expenditures.[13] To that end, DS is committed to evolving our current infrastructure into an improved PCN. Cloud computing is a style of computing in which scalable and elastic IT-enabled capabilities are delivered as a service to external customers using internet technologies.[14] The PCN, founded on JWICS, is critical to gaining mission and cost efficiencies immediately on TS/SCI networks and delivering intelligence information faster and more cheaply through the PCN's common infrastructure. Enhancing the PCN will expand DoDIIS's flexibility by enabling capacity to be added or removed quickly, based on shifting user demand. The PCN will facilitate information sharing by transforming the current DoDIIS IT infrastructure into an agile, mission-centric environment. DS will:

- Evolve the current infrastructure to a scalable and flexible PCN infrastructure to respond to changing customer demand and enable quicker, easier, information sharing across DoDIIS.
- Provide the flexible computing power necessary to increase operational excellence and meet evolving requirements.
- Create budget and operational efficiencies by centralizing network control under DS.

1.2: Provide access to tools and information across different network and security domains.

Our customers must collect information and leverage tools from across the defense intelligence community, around the globe, and from tactical to strategic levels to effectively execute their missions. Currently, defense intelligence agencies, combatant commands, and military services have their own separate networks and data repositories. Separate networks make it difficult to access tools and piece together facts and suppositions that in the aggregate could provide forewarning of threats.[15] DS must provide seamless access to these tools and

information across different domains regardless of organization ownership and security level. Seamless access to information will facilitate communication and understanding with mission partners and allow customers to synthesize information more quickly and easily and create a decision advantage. DS will:

- Manage and deliver intelligence information and tools to our customers across multiple classification domains.
- Set and facilitate the application of consistent standards and protocols to ensure interoperability between systems and applications across DoDIIS and in the cross-IC Common Operating Environment (COE).

1.3: Cultivate an environment in which members of DoDIIS routinely practice information sharing.

At its heart, information sharing is a behavior facilitated by technology.[16] To encourage information sharing, DS must cultivate an environment in which people routinely share information out of ease and obligation. DS must influence the development of legislation and directives that achieve information sharing and security by regulating technology advancements.[17] DS will encourage its employees to practice information sharing across the directorate and with external mission partners by fostering a "responsibility to provide" culture and influencing necessary policy and authority changes.[18] DS will:

- Emphasize the value of sharing information and expand awareness of information sharing capabilities through release of DS-wide communications.
- Encourage information sharing by aligning compensation, performance objectives, and incentives around the behavior.
- Train workforce and customers on information sharing practices and tools.
- Advocate for relevant policy changes through partnerships with peer agencies and policymakers.

Goal 2: Achieve World-class IT Security and Collaboration across Multiple Networks

Internal and external security threats change rapidly as our enemies create new methods to compromise our IT systems. DS will provide a world-class security infrastructure and evolve its methods to protect the defense intelligence IT infrastructure from capable aggressors.

DS will achieve security and facilitate information sharing, collaboration, and access to our portfolio of tools and services across multiple classification levels.[19] Today's mission requires intelligence information from across agency lines and classification levels. However, classified networks are numerous, complex, physically separate, and differ across agencies. Members of the defense intelligence community must log on to multiple machines and transfer information across networks to execute their mission.[20] The exchange process is time consuming and delays information from reaching users who need it.

To meet mission needs, DS will build a security infrastructure to defend against threats in a dynamic network environment. DS will provide access between multiple secure networks by implementing persona-based access and influencing necessary policy changes.

2.1: Build a security infrastructure to defend against threats in a dynamic network environment.

Defense intelligence systems and networks are constantly under attack. Fortifying our systems and networks is difficult because as IT needs expanded, organizations independently developed IT infrastructures with unique standards and security provisions. A given network's weak security procedures can place DoDIIS' infrastructure at risk. To remedy this, DS will build a holistic security infrastructure including physical, network, cyber, and information security to secure defense and intelligence networks from threats. DS will:

- Assess and manage security risks and vulnerabilities inherent in protecting the nation's most sensitive information.
- Build physical security infrastructure for the PCN to protect hardware, programs, and data from damage or loss.
- Develop network and cyber security capabilities to detect and defend the network against internal and external threats.
- Manage security configurations and automate compliance monitoring and enforcement.

2.2: Securely connect multilevel security domains utilizing persona-based access.

DoDIIS uses multiple classified, physically separate networks to achieve mission goals. Members of DoDIIS must log in to multiple networks in order to access necessary information. Additionally, individuals have to forego access to certain tools that are limited to specific networks.[21] This process delays intelligence information from reaching those who need it. DS will increase delivery speed of critical mission services by maintaining distinct and physically connected networks that individuals will access through persona-based access. Users on one network will be able to connect to another network and access tools and information more easily because of reduced time required to log in to multiple networks. An individual's unique persona and clearance level will determine his or her level of access to information and tools. This will save time, money, and facilitate information sharing.

DS will:

- Assess the solution gaps on JWICS, SIPR, NIPR and across TS/SCI networks.
- Bridge physical division of classified networks.
- Implement persona-based identity access management across its user base.

2.3: Influence evolution of policies and authorities.

Transforming the IT infrastructure in the defense intelligence community requires changes beyond technology. Historical IT infrastructure is the basis for current policies and authorities and therefore limits future development of IT.

As the defense intelligence community progresses to meet evolving mission needs and leverages technology, IT policies and authorities must also evolve to remain relevant and current. Specifically, policy changes are required to build the PCN, support access to multiple networks, and implement persona-based identity management. DS will:

- Identify policy gaps that impact implementation and adoption of PCN capabilities, connecting networks, and persona-based identity management.
- Work with mission partners to influence relevant IT related policies.

Goal 3: Develop the DS Workforce

DS will face greater challenges as the organization and mission expand to address changing technology and security threats. The DS workforce is the key to successful execution of the DIA and DoDIIS mission. DS staff is responsible for executing the mission on a day-to-day basis while planning for and progressing towards the DS Strategic Vision. The mission challenges of the next two to five years will require diverse intellectual perspectives and a broad range of skills. DS will shape the workforce for the future by developing current employees and recruiting new talent.[22]

By shaping the DS workforce and enhancing technology, DS will contribute to developing IT skills across DoDIIS. As this community utilizes the enhanced technology provided by DS, such as self-service, collaboration tools, etc, they will develop their skills and abilities to achieve optimal performance.

3.1: Develop workforce skills and expertise necessary to execute our Strategic Vision and build the next generation of technology leadership for DoDIIS.

DS will establish and operate a training program for DS employees. The DS workforce needs adequate training, tools, and opportunities to refresh skills, develop new competencies, and prepare for leadership roles. Talented junior employees can draw on their valuable training and experiences to become the next generation of DS leaders, as our current workforce retires. The training and experience working with DS will also equip select employees to lead the broader DoDIIS community's technology growth in a rapidly changing environment.

In order to maximize growth potential for employees, DS will:

- Align employees' Individual Development Plans (IDPs) and yearly objectives to the DS Strategic Vision and Career Path Guides [23]
- Optimize current workforce skills and abilities by providing regular and relevant training opportunities and experiences to individuals at all levels

3.2: Recruit diverse talent necessary to increase depth and breadth of workforce capabilities to address future needs.

While DS' current workforce possesses skills and competencies to meet today's demands, the future will require new capabilities. DS will build its workforce by recruiting individuals with appropriate skills and knowledge to replace departing employees, in addition to training current employees in critical skills. DS will:

- Attract talent by establishing a new talent value proposition centered on the unique opportunities at DS to contribute to national security and develop advanced technology.
- Secure top talent efficiently and effectively by identifying key sources of talent and executing a focused recruitment strategy.
- Supplement workforce with contractors to address the need for rapidly changing IT skills.
- Enhance new employees' ability to be productive, high performing contributors to the mission by developing and implementing

a DS-specific new hire integration program to complement DIA's Gateway orientation.

3.3: Enhance the DS work environment and improve employee satisfaction.

DS needs to retain satisfied employees who it can invest in to build the next generation of DS leaders. Establishing and maintaining high employee morale and satisfaction creates tremendous benefit for any organization, as satisfied and enthusiastic employees have greater commitment to DS and are more effective mission executers. There are many factors in improving high employee satisfaction and lowering employee turnover. DS will take a holistic approach to employee satisfaction by reviewing and enhancing the employee culture, employee quality of life, policies and tools employees use to execute their work, and the overall value proposition of working for DS. DS will:

- Regularly survey employees to measure satisfaction across broad categories and resolve issues that affect quality of life.
- Develop and enhance the tools and capabilities employees use to complete work and collaborate.
- Retain talented people by emphasizing the unique and meaningful value of an opportunity to contribute to national security and develop advanced technology.
- Foster long-term employee investment in DS' future by providing transparency into leadership and organization direction.

Goal 4: Operate Effectively and Efficiently

We must meet our customer and internal mission needs without fail; U.S. national security depends on DS. In order to understand and meet customer needs effectively, DS must build trust as a mission partner. A mission partner goes beyond traditional desktop and network support, fully understands and aligns to its customers' agenda, and works in partnership to provide the most relevant and timely comprehensive technology solutions to enable mission execution. DS will earn a reputation as a mission partner by consistently delivering on customers' expectations and enhancing customer service during support interactions. DS understands holistically what it takes to become a mission partner and will work diligently to enhance customer trust.

While our commitment to our customers is endless, our resources are limited. DS must meet our customers' mission by being good stewards of taxpayer resources and operating efficiently. DS must also enable IT efficiencies throughout DoDIIS since information technology has been one of the great levers for lowering operating costs. Improving efficiency and effectiveness will help us excel at our own mission, and enable others to perform theirs, faster, with higher quality, and at a lower cost. We will execute our mission with operational excellence. DS will steward IT resources through its control of the IT budget.

Effectiveness: Increase customer satisfaction

4.1: Achieve consistently higher levels of customer satisfaction by building customer trust.

DS is a customer-centric organization dedicated to working with DoDIIS as a mission partner. Our promise to our customers is, "Committed to mission and partnership, DS meets your IT needs." As such, customer satisfaction is a key measure of DS' mission success. Building trust is at the crux of improving customer satisfaction with DS. Customers across DoDIIS most value working with a trustworthy IT organization; an organization they can rely on to deliver consistent products and services that work and respond to their needs.[24] Given customers' emphasis on trust, DS must enhance customer relationships by earning credibility and building trust at both the enterprise level and through individual interactions.[25] DS will build trust in two ways. First, DS will consistently offer effective, reliable, products and service to meet customers' mission needs. DS will also establish greater transparency into available products and service request fulfillment, thus clarifying expectations and creating visibility into DS performance. Trust is the foundation of mission partnership. Earning and keeping the right to be a mission partner requires understanding customer needs and proactively partnering with customers during early mission phases to execute mission priorities. DS will:

- Set customer experience expectations by establishing service level commitments and measuring, synthesizing, and communicating DS progress against service levels.
- Provide effective products and customer service that meet customer needs.
- Release communications that encourage customers to adopt new products and services.

4.2: Build reputation for service excellence.

In order to be given the opportunity to team with customers, customers must believe that DS will effectively and consistently provide

mission necessary IT services. DS' reputation must be strong enough to support this belief. To strengthen our reputation, we will deliver proactive, timely, knowledgeable, and professionally courteous customer service that our customers across DoDIIS desire. DS will design timely and effective customer service interactions for each type of customer, with clear business rules and expectations. We deliver these consistent customer experiences in order to build trust and exceed customer expectations. DS will:

- Design and implement efficient and effective customer service interactions.
- Infuse customer importance factors into service processes for each customer interaction channel.
- Deliver consistent professional frontline service.
- Prioritize mission critical service requests.
- Fulfill service requests on time or earlier to meet and exceed customer expectations.
- Develop a robust self-service support tool to save customers time and effort necessary to request support.
- Build help desk capacity for customers who seek face-to-face or telephone support.
- Consistently deliver services across all regions.

Efficiency: Achieve our mission with decreased funding by resourcefully leveraging internal assets and improving productivity.

DS has an enduring duty to use taxpayer resources wisely, never forgetting that we work on behalf of American citizens. Organizations frequently use information technology to generate significant operating efficiencies. DS will lead DoDIIS in taking advantage of new technology to continuously reduce cost and improve productivity, both internally within DS and DIA and in our customer organizations.[26]

4.3: Enhance IT operational efficiency.

DS is committed to using taxpayers' dollars efficiently to progress the mission of DoDIIS. DS will use resources more efficiently by seeking greater mission benefit from existing technology assets and reforming our business processes. Currently, the disparate systems and networks of DoDIIS involve significant maintenance and upgrade costs. Implementing shared cloud computing technology and services as well as providing increased cross-domain access to common products are two key initiatives to leveraging economies of scale to increase buying power. These initiatives will also reduce redundant efforts and costs associated with IT development and operation across DoDIIS. Moreover, in line with the Federal CIO's efforts to reduce data centers, DS will continue consolidating data centers to gain cost savings and contribute to creating a greener IT infrastructure. In addition, DS will:

- Regularly review how we operate at the leadership level to find step change improvements in operations, processes, and asset utilization.
- Commit to an effective continuous process improvement program so that we constantly identify and capture small and large ways to execute the mission better, faster, and cheaper.

4.4: Improve customer productivity.

In addition to capturing efficiencies internal to DS, we will also help our customers identify and capture efficiencies. First, DS will continuously identify, share, and help implement IT tools that speed operations, improve collaboration, improve workflow, and reduce costs. Providing cloud-computing services to facilitate information sharing and enabling increased cross-domain access to technology solutions are examples of how DS will improve employee productivity. Our role also extends to helping customers reduce waste and complexity. In this context, providing standard products and services to meet customer needs is a critical part of how DS will build trust and advance DS' relationship with its customers,

while also reducing operating costs. DS customers desire reliable basic desktop and network solutions, in addition to expecting DS to deliver on their unique needs.[27] These needs are even more pronounced at the edge, defined as those places in the world where DS customers are actively engaged in enforcing or protecting U.S. foreign policy at the tactical level. DS is committed to understanding customer needs and helping them work effectively and efficiently. DS will:

- Deliver a reliable desktop experience by assigning DS resources to priority projects focused exclusively on the desktop experience.
- Provide simple tools that customers can easily understand and use.
- Offer training aids and demos to help customers understand how to use more complicated products and services.
- Refine products based on customer feedback.
- Improve most frequently used software and hardware with timely and easy to use upgrades.
- Update product list frequently with a variety of relevant offerings that enable mission needs.
- Release new products quickly based on priority requests and urgent requirements.
- Meet unique customer needs at the Edge by providing updated, reliable, equipment.

4.5: Optimize geographic disbursement of workforce and capabilities.

Information technology plays an important role in helping organizations efficiently surmount time and space constraints. This is important as the DS and DIA workforces are geographically disbursed. DS' role is to provide communication, collaboration, and mission tools that reduce or eliminate the inefficiencies associated with operating in multiple work locations. On behalf of the agency, we will help implement solutions that help us and our customers accomplish missions effectively, regardless of time and physical location considerations. DS will:

- Provide effective communication and collaboration tools based on assessment of customer needs.
- Tailor products for employees working in unique situations.

Conclusion

The United States faces rapidly changing threats. To counter these threats and stay one step ahead, DoDIIS' IT tools must enable the IC to quickly and securely collect, share, assess, and disseminate information from a variety of sources that span multiple agencies and classification levels. The DS Strategic Vision outlines how DS will advance the technical capabilities of DIA and DoDIIS. DS will transform DoDIIS technology infrastructure to facilitate secure collaboration and information sharing, resource goals with human capital expertise, and fulfill our mission effectively and efficiently.

The DS Strategic Vision describes goals that are thoughtful, actionable, and measureable. They lead to outcomes that help address defense intelligence community concerns and fulfill the DS mission. DS must now translate these strategic goals into initiatives, plans, and capabilities. Decisions about budgeting, programs, operations, and acquisition will reflect the direction provided by the DS Strategic Vision.

Ultimately, DS will establish the OSE that hosts multiple levels of classified information. DS will also be able to define and designate defense intelligence IT as a weapons system, enabling DS to meet policymakers' and warfighters' evolving needs and continue to defend our nation.

Through its technical capacity and dedication to its customers, DS will enable DoDIIS to securely share information in order to be agile and responsive to the full spectrum of threats and preserve America's intelligence technology advantage.

Acronyms and Terms List

Cloud	Model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.[28]
COE	Common Operating Environment
DIA	Defense Intelligence Agency
DoDIIS	Department of Defense Intelligence Information System
DoD	Department of Defense
DS	Directorate for Information Management and Chief Information Officer, DIA
IC	Intelligence Community
OSE	One Secure Environment
PCN	Private Cloud Network

Endnotes

1. President Barack Obama, "Remarks By The President On Securing Our Nation's Cyber Infrastructure" (speech, White House, Washington, DC, March 05-29, 2009), *http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure.*

2. Defense Intelligence Agency, 2012-2017 Defense Intelligence Agency Strategy (Washington, DC, 2011) Goal 3: Objective 3.3

3. U.S. Office of the Director of National Intelligence, United States Defense Intelligence Strategy (Washington, DC, 2008), *http://merln.ndu.edu/archive/NSS/strategies/DefenseIntelligenceStrategy08May.pdf.*

4. U.S. Office of the Director of National Intelligence, United States Defense Intelligence Strategy (Washington, DC, 2008), *http://merln.ndu.edu/archive/NSS/strategies/DefenseIntelligenceStrategy08May.pdf.*

5. U.S. Department of Defense, Joint Publication 6-0 – Joint Communications Systems (Washington, DC, 2010), II-2.

6. U.S. Office of the Director of National Intelligence, United States Intelligence Community Information Sharing Strategy (Washington, DC, 2008), *http://www.dni.gov/reports/IC_Information_Sharing_Strategy.pdf,* 3.

7. U.S. Department of Defense, Joint Publication 6-0 – Joint Communications Systems (Washington, DC, 2010), II-2.

8. U.S. Office of the Director of National Intelligence, United States Intelligence Community Information Sharing Strategy (Washington, DC, 2008), *http://www.dni.gov/reports/IC_Information_Sharing_Strategy.pdf,* 11.

9. Report of the United States Senate Select Committee on Intelligence, Attempted Terrorist Attack on Northwest Airlines Flight 253. (Washington, DC U.S. Government Printing Office, May 24, 2010)

10. Mortimer Zuckerman, "How to Fight and Win the Cyberwar," The Wall Street Journal, 6 December 2010, *http://online.wsj.com/article/SB10001424052748703989004575652671177708124.html.*

11. Defense Intelligence Agency, 2012-2017 Defense Intelligence Agency Strategy (Washington, DC, 2011) Goal 3: Objective 3.1-3.2.

12. U.S. Office of the Director of National Intelligence, United States Intelligence Community Information Sharing Strategy (Washington, DC, 2008), *http://www.dni.gov/reports/IC_Information_Sharing_Strategy.pdf,* 8.

13. Jim Garamone, "Gates Puts Meat on Bones of Department Efficiencies Initiative," American Forces Press Service (U.S. Department of Defense), (2010), *http://www.defense.gov/news/newsarticle.aspx?id=60348.*

14. Thomas J. Bittman, "Private Cloud Computing: An Essential Overview," Gartner Research, (2010).

15. Defense Intelligence Agency, 2012-2017 Defense Intelligence Agency Strategy (Washington, DC, 2011) Goal 1: Objective 1.1-1.2.

16. U.S. Office of the Director of National Intelligence, United States Intelligence Community Information Sharing Strategy (Washington, DC, 2008), *http://www.dni.gov/reports/IC_Information_Sharing_Strategy.pdf,* 18.

17. U.S. Office of the Director of National Intelligence, United States Intelligence Community Information Sharing Strategy (Washington, DC, 2008), *http://www.dni.gov/reports/IC_Information_Sharing_Strategy.pdf,* 8.

18. U.S. Office of the Director of National Intelligence, Intelligence Community Directive 501 (Washington, DC, 2009), *http://www.dni.gov/electronic_reading_room/ICD_501.pdf,* 2.

19. Defense Intelligence Agency, 2012-2017 Defense Intelligence Agency Strategy (Washington, DC, 2011) Goal 1: Objective 1.2.

20. U.S. Office of the Director of National Intelligence, United States Intelligence Community Information Sharing Strategy (Washington, DC, 2008), *http://www.dni.gov/reports/IC_Information_Sharing_Strategy.pdf,* 3.

21. U.S. Office of the Director of National Intelligence, United States Intelligence Community Information Sharing Strategy (Washington, DC, 2008), *http://www.dni.gov/reports/IC_Information_Sharing_Strategy.pdf,* 3.

22. Defense Intelligence Agency, 2012-2017 Defense Intelligence Agency Strategy (Washington, DC, 2011) Goal 2: Objective 2.2-2.3.

23. Defense Intelligence Agency, 2012-2017 Defense Intelligence Agency Strategy (Washington, DC, 2011) Goal 4: Objective 4.1.

24. U.S. Defense Intelligence Agency, Directorate for Information Management and Chief Information Officer, DS Voice of the Customer Survey 2010 Analysis (Washington, DC, 2010).

25. U.S. Defense Intelligence Agency, Directorate for Information Management and Chief Information Officer, DS Voice of the Customer Survey 2010 Analysis (Washington, DC, 2010).

26. Defense Intelligence Agency, 2012-2017 Defense Intelligence Agency Strategy (Washington, DC, 2011) Goal 3: Objective 3.3.

27. U.S. Defense Intelligence Agency, Directorate for Information Management and Chief Information Officer, DS Voice of the Customer Survey 2010 Analysis (Washington, DC, 2010).

28. U.S. National Institute of Standards and Technology, Definition of Cloud Computing, (Washington, DC, 2008), 1, *http://csrc.nist.gov/groups/SNS/cloud-computing/.*

For More Information

Defense Intelligence Agency
Directorate for Information Management and CIO
200 MacDill Blvd., Building 6000
Washington, DC 20340-0001
(202) 231-6068 | *www.dia.mil*

JWICS
http://www.dia.ic.gov/admn/ds/index.html

SIPR
http://www.dia.smil.mil/admin/ds

DIA protects the environment while protecting the nation.

PCN 27610