



---

# **National Guard Bureau**

# **Chief Information Officer / J6**

---

## **500 Day Plan**

**February 2020**



## Mr. Kenneth C. McNeill, SES, National Guard Bureau CIO/J6

### Director's Comments



I am extremely proud to present the FY 2020-2021 Chief Information Officer (CIO) National Guard Bureau (NGB) 500 Day Information Technology (IT) Plan. The NGB is continuing its transformational journey to better serve our nation in support of both domestic operations (DOMOPS) and warfighting missions.

We face an ever-changing and challenging IT environment. Our IT mission requirements span across our traditional Title 10 role as a critical warfighting component in support of the active Army and Air Force to the Title 32 role of domestic operations, in support of the 50 States, 3 Territories and the District of Columbia and the 54 JFHQ-S.

The NGB CIO/J6 Directorate is actively engaged every day to help shape IT activities and support the unique mission requirements of the National Guard. The directorate represents the National Guard command, control, communications, and computers/cyber (C4) requirements validation and capability development processes while ensuring interoperability. To further this effort, the NGB CIO/J6 promulgates policy/governance and provides functional expertise to the Chief, of the National Guard Bureau (CNGB) in order to shape the Joint Information Environment (JIE) in support of the 54.

This 500-Day Plan guides our NGB CIO/J6 Directorate leaders and workforce in making informed decisions by providing direct focus on the key NGB CIO/J6 IT initiatives while working to synchronize the efforts of the IT community across the National Guard. These key initiatives are directly aligned to specifically established Lines of Effort (LoEs) aimed at achieving specific goals over the next 500 days.

We must continually assess our priorities to ensure that our NGB CIO/J6 IT initiatives align with the Department of Defense (DoD) strategic initiatives and IT reform programs. This plan is aligned to the DoD's Digital Modernization Strategy which addresses four focus areas: Cybersecurity (CS), Artificial Intelligence (AI), Cloud Computing Environment (Cloud), and Command, Control, and Communications (C3).


We must be innovative in our approach to ensure that we manage IT investments efficiently to meet the desired effect across our mission requirements. Innovation is one of the CNGB's top priorities, and we will use innovative IT solutions in close coordination with Air National Guard (ANG) and Army National Guard (ARNG) to effect change in a meaningful way by increasing efficiencies and strengthening productivity.

The NGB CIO/J6 Directorate is on the leading edge of orchestrating world-class IT capabilities and services for the National Guard (NG) joint community, Joint Force Headquarters Staff (JFHQ-S) at every State, and interoperability with our mission partners when called upon.

As we modernize the NG's digital environment, we must recognize now more than ever the importance of collaboration with our industry and service partners. Wherever possible we will leverage our industry partner's expertise and innovation to increase IT capability across the NG.

These are trying times in a fiscally constrained environment and the way ahead will not be easy. However, it is also an exciting time for the men and women of the NG fortunate enough to serve and play a vital role in the future success of this organization. The NGB CIO/J6 Directorate will work diligently to meet the distinct IT challenges that are before us in support of our global and domestic missions.

I expect the senior leaders and staff of our directorate to understand my intent and guidance in this 500-Day plan and use it to drive the implementation of key projects to successfully improve IT capability in support of the NG. Furthermore, the NGB CIO/J6 Directorate will use this Plan to align and synchronize our efforts for IT related activities over the next 500 days.

  
Kenneth C. McNeill  
Chief Information Officer /J6  
National Guard Bureau

## Table of Contents

<b>I. What Guides Us</b> .....	<b>1</b>
<b>II. NGB CIO/J6 Mission, Vision, and Guiding Principles</b> .....	<b>5</b>
<b>III. NGB CIO/J6 IT 500 Day Plan - Lines of Effort</b> .....	<b>7</b>
<b>IV. NGB CIO/J6 Organizational Structure</b> .....	<b>9</b>
<b>V. Deputy CIO/J6</b> .....	<b>11</b>
<b>VI. J63, C4 Operations Division</b> .....	<b>13</b>
<b>VII. J65, Strategy and Policy Division</b> .....	<b>18</b>
<b>VIII. Closing Remarks</b> .....	<b>23</b>
Appendix A. References .....	24
Appendix B. Acronyms .....	25
Appendix C. NGB CIO/J6 Directorate Key 500 Day Goals .....	28

# I. What Guides Us

As described in the President’s National Security Strategy (NSS), the Government’s fundamental responsibility is to protect the American people, the homeland, and the American way of life. A country that is strong and prosperous at home is a country capable of defending its interests and advancing its influence abroad. While America possesses enduring national strengths, we face an era of increased strategic competition, global challenges, and erosion of the U.S. comparative military advantage. In addition to the global challenges, NG Soldiers and Airmen support the needs of the Nation, the Army, and the Air Force as an operational warfighting force providing strategic depth. This support captures a balance of combat and enabling units that largely mirror our active Army and Air Force. The current threat environment blurs the lines between domestic and overseas threats. Current examples of these challenges include the National Guard support at the Southwest border and Cybersecurity in support of the 54. The NG’s versatility enables tailored responses to domestic emergencies, overseas combat missions, counterdrug efforts, Cybersecurity protection at the state level, and more. In order to preserve peace through strength, we must continue to invest in combat credible military capabilities increasing our lethality in order to compete, deter, and if necessary, fight and win wars.



Figure 1: NG Strategic Road Map/Framework

Figure 1 provides a depiction of the national defense strategic framework and its relationship to foundational NGB strategic documents. As displayed, strategic planning begins at the Executive level and becomes more refined as it develops. The 2018 *National Defense Strategy* (NDS) outlines the primary NDS LoEs – *to build a more lethal force, strengthen alliances, attract new partners, and reform the Department of Defense for greater performance and affordability, and individual fundamentals*. See Figure 2. The NDS informs the *National Military Strategy* (NMS) however; given the unique mission set of the NG, the NMS is only applicable to NG Soldiers and Airmen while working in their Title 10 role as active duty Air Force and Army personnel. The NGB is the focal point at the strategic level for non-federalized NG matters that are not the responsibility of the Secretary of the Army, the Secretary of the Air Force, or the Chairman of the Joint Chiefs of Staff (CJCS), in law or DoD policy.

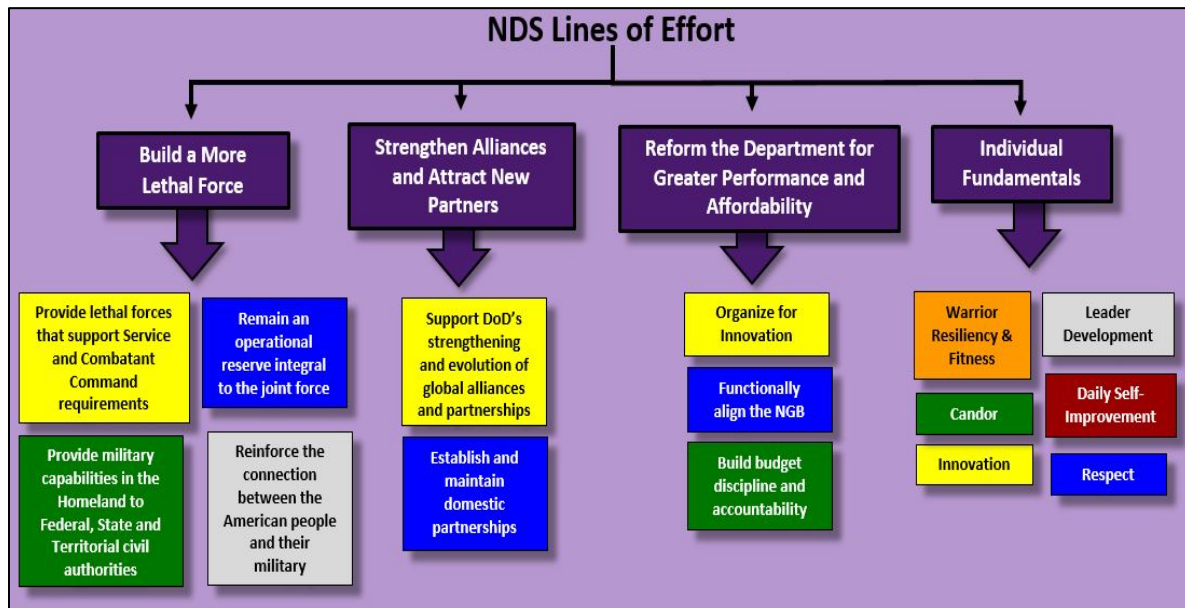


Figure 2: National Defense Strategy LoEs

The NG Strategic Road Map in Figure 1 centers upon the understanding and realization that, given a lack of control regarding resources, a traditional ends, ways and means approach is not suited for the National Guard. The CNGB approved a methodology and approach that compensated for this factor by not using the word “strategy” in the traditional sense. Instead, the strategic approach included the development of the *National Guard Strategic Estimate* (NGSE) and the *National Guard Posture Statement*, which define and explain the nature of National Guard support to current global and domestic challenges. These two documents precede the development of the *National Guard, National Defense Strategy (NDS) Implementation Guidance*, which outlines the strategic direction, guiding policy, and individual fundamentals that enable the success of the National Guard.

All of these documents constitute the strategic framework used to support the diagnosis, guiding policy and development of the *National Guard Bureau Strategic Plan* (NGBSP). The NGBSP is the culminating document, which essentially establishes how the National Guard will meet strategic objectives. It's the final document developed to establish priorities across lines of effort

**NGB Mission** - The CNGB focuses every day on accomplishing three core missions – fighting America's wars (**Warfighting**), securing the homeland (**Homeland**), and building enduring partnerships (**Partnerships**)

2019 NGB Posture Statement Pg. 4

while synchronizing the timing of objectives. The CNGB is focused every day on accomplishing three core missions; *fighting America's wars, securing the homeland, and building enduring partnerships*. Figure 3 portrays how the NGB's core mission areas nest under the NDS's LoEs. The NGB accomplishes its mission through a combined effort and directly supports the NDS's LoEs: *building a more lethal force, strengthening alliances and attracting new partners, reforming the DoD for greater performance and affordability, and individual fundamentals*.

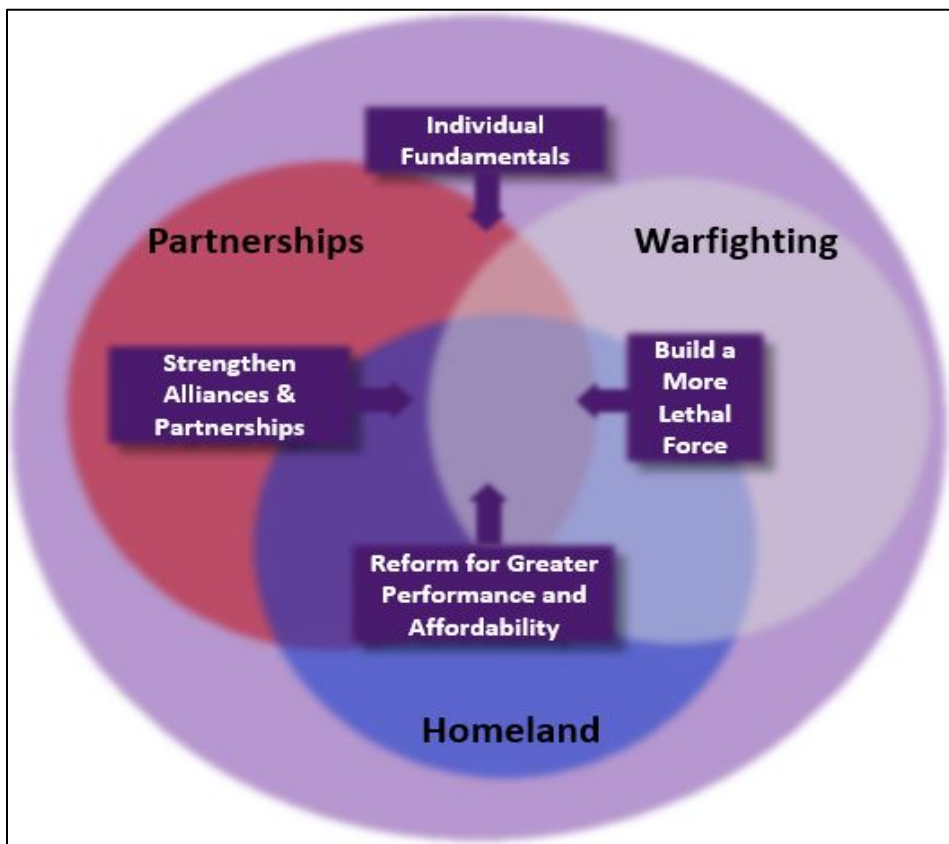


Figure 3: NDS's LoEs and NGB Core Mission Areas

Nested under the NDS's LoEs, the DoD CIO is currently pursuing alignment reform in accordance with the 2019 *DoD Digital Modernization Strategy* to include "Innovation for Advantage" and "Resilient Cybersecurity", both key components of the NDS's initiative for



reform. In addition to the Strategic Framework outlined in Figure 1, the NGB CIO/J6 Directorate is also aligning to the DoD strategic initiatives outlined in the DoD's Digital Modernization Strategy. As we continually assess our priorities, we must ensure that our initiatives align with the DoD strategic initiatives. The DoD's Digital Modernization Strategy provides direction on the four core focus areas: Cybersecurity (CS), Artificial Intelligence (AI), Cloud Computing Environment (Cloud), and Command, Control, and Communications (C3).



---

*A National Guard Soldier watches a row of monitors in the communications department of the Yuma Sector Border Patrol Station in Arizona. The Soldier is assigned to the Wisconsin Army National Guard.*

---

## II. NGB CIO/J6 Mission, Vision, and Guiding Principles

*The NGB CIO/J6 Mission: Lead the NG Joint IT community's Command, Control, Communications, and Computers (C4), and Cyber capability initiatives. Provide the NGB and the 54 with IT policy, plans, strategy, and guidance. Maintain effective IT capabilities across the NG's joint, domestic, and mission partner domains.*

### **CIO/J6 VISION**

**Provide secure and interoperable enterprise IT capabilities, both tactical and strategic, in support of NGB's Domestic and Warfighting Missions**

In support of the NGB mission, the NGB CIO/J6 establishes policies and procedures, provides advice, and makes recommendations on J6 matters to the CNGB, ANG, and ARNG. We support the Combatant Commands, interagency, and JFHQ-S information sharing for the homeland security mission. The NGB CIO/J6 vision serves as a guide for all of the NG CIO/J6 priorities. These priorities directly align with the NDS. By meeting these priorities, the NGB will move closer to achieving the CNGB goals outlined in the 2020 Posture Statement.

The NGB CIO/J6 will also develop a NGB long term IT strategy, and plan in support of C4 programs, portfolio management, and Artificial Intelligence (AI) for example, all used in a trusted, shared environment across the ARNG and the ANG.

In order to achieve the NGB CIO/J6 vision and mission in a synchronized effort, three guiding principles were established: *perform the mission, work as a team, and continually improve* were established. The term "guiding" refers to the fact that these principles and values are established to lead the organization in any situation it might face. These guiding principles are essential in the decision-making processes and crucial for the successful operation of the organization. Therefore, every member of the organization must have a clear understanding regarding the framework of these principles.

# **NGB CIO / J6 Guiding Principles**

## **Perform the mission**

- Deliver world-class IT support for the CNGB, NG community, the JFHQ-S, and our mission partners
- Share and manage information among the combatant commands, States, and interagency partners
- Establish, maintain, and coordinate Shared Situational Awareness (SSA) of all NG assets among NG stakeholders and users
- Employ emerging technologies to permit the interface between Federal, State, and civil emergency response teams as required
- Continually seek innovative ways to enhance IT capabilities in support of Federal and non-Federal mission requirements
- Be a subject matter expert in your career field and a valued and productive member of the J6 team.

## **Work as a team**

- Ensure everyone is treated with dignity and respect, regardless of title or position
- Creativity is the lifeblood of our organization – it must be encouraged at all levels
- We are all responsible for making the NGB CIO/J6 a safe workplace, inclusive of others, and where everyone should be comfortable voicing ideas
- We must communicate constructively and always be open and transparent

## **Continually improve**

- Customer service – Support all users
- Improve processes and performance measures to ensure effective outcomes
- Opportunities for professional growth

These guiding principles will help our CIO/ J6 team members understand how to function as a successful team. They set the standards and expectations for our team members to meet. These Guiding Principles will facilitate the value of good teamwork, coordinated staff actions, enabling the delivery of the best IT capabilities and products possible.

### III. NGB CIO/J6 IT 500 Day Plan - Lines of Effort

The NGB CIO/J6 IT 500 Day plan outlines key goals for the directorate in order to establish the process for managing the implementation of IT-related initiatives. This will help accelerate IT capability delivery, efficiency, and effectiveness in support of the National Guard mission and objectives. The 500-Day plan supports the NGB CIO/J6 leadership and staff in their ability to manage IT-related initiatives. It supports the development of an implementation plan, which will facilitate the management of key NGB CIO/J6 IT goals and projects. Given the complex nature of the NG and NGB CIO/J6 activities, the directorate created LoEs to clarify, synchronize, and focus CIO/J6 operational and strategic initiatives. Figure 4 identifies the six CIO/J6 LoEs, and a supporting effort, nested within the NDS's LoEs and the CNGB's core mission areas.

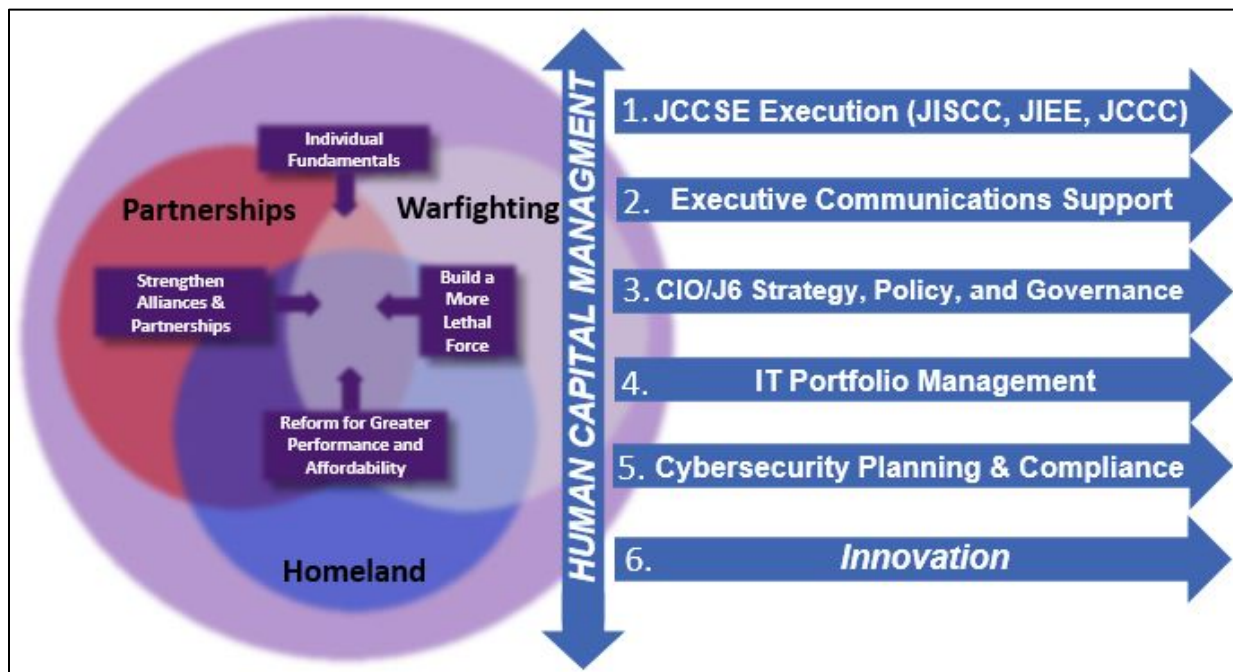
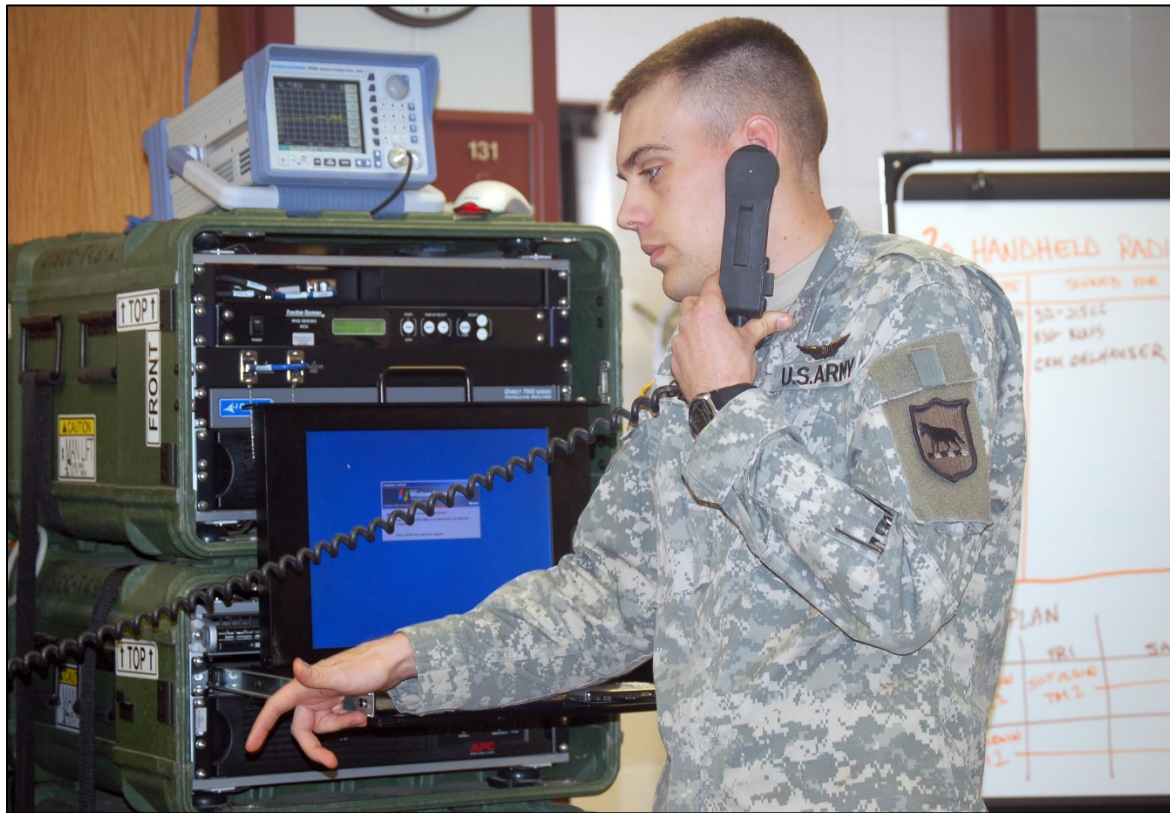


Figure 4: NGB CIO/J6 LoEs

After careful analysis and prioritization of key tasks and initiatives, the six LoEs became the focus areas for the directorate. Each division is responsible for its corresponding LoEs. This helps to focus and coordinate the implementation of key IT activities across the directorate. Depicted vertically in the diagram, Human Capital Management is a supporting effort. It is not an identified LoE; however, its critical functions of manpower/personnel management, Planning, Programming and Budget Execution (PPBE) and contract management are critical to the success of all designated LoEs.

As a result of the LoEs, each division created specific 500-Day key goals. These key goals are benchmarks and enable the J6 to measure the progress and success of the NG and CIO/J6 Directorate over the next 500 days.



---

Sgt. Chris A. Olson, with the South Dakota National Guard's Joint Force Headquarters, operates the Joint Incident Site Communications Capability (JISCC) system. The system allows Soldiers and Airmen to communicate with emergency responders on the ground.

---

# IV. NGB CIO/J6 Organizational Structure

The CIO/J6 team consists of over 75 military, civilian, and industry partners operating across two divisions and six branches, led by a CIO/J6 Director (SES) and Deputy Director.

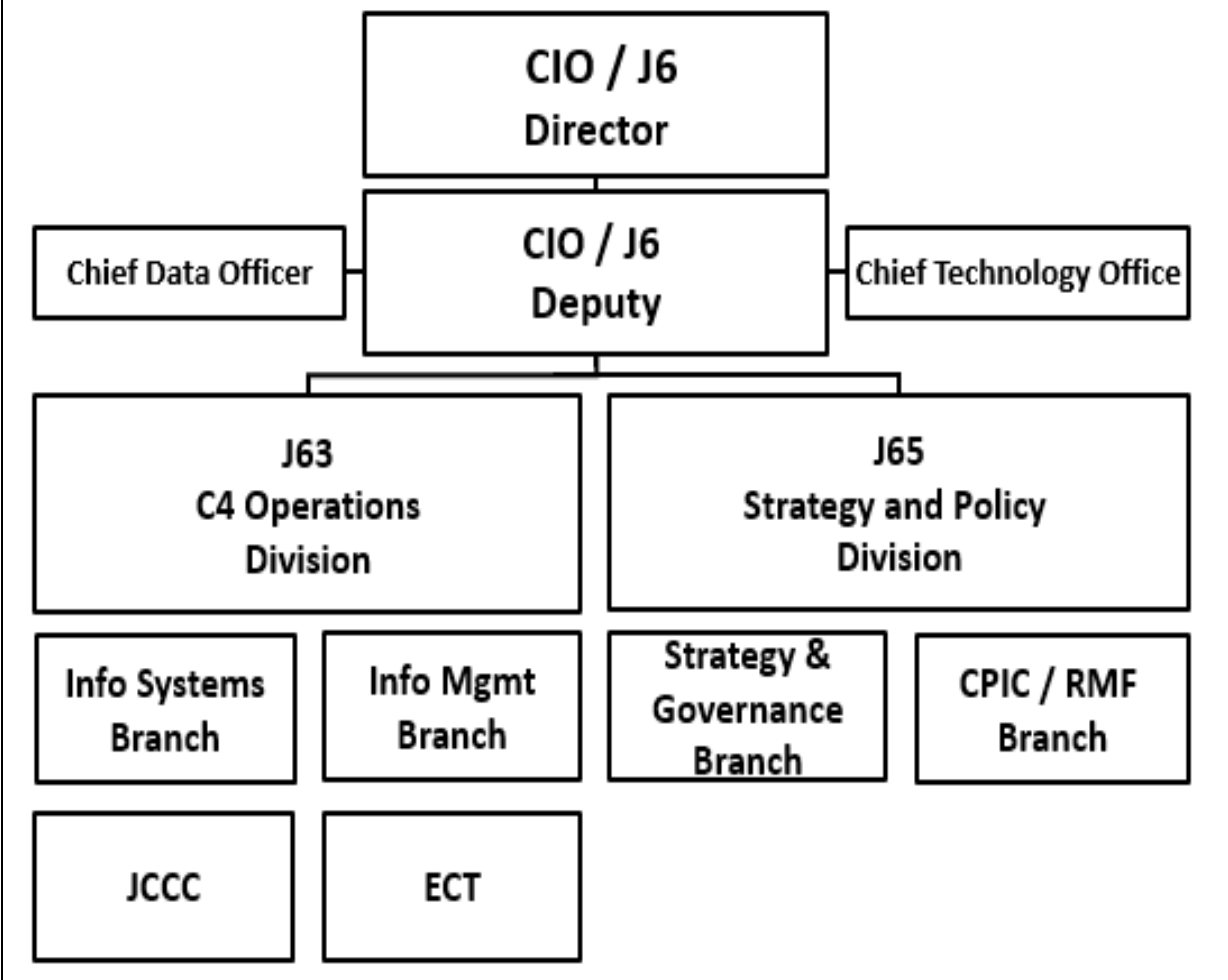


Figure 5: NGB CIO/J6 Directorate

**The CIO/J6 Director**

The Director is responsible for advising the CNGB on Command, Control, Communications, and Computers (C4), and Cyber capability initiatives. Additionally, the Director provides the NGB and the 54 with IT policy, plans, strategy, and guidance while maintaining effective IT capabilities across the NG’s joint, domestic, and mission partner domains.

### **The CIO/J6 Deputy Director**

The Deputy Director is responsible for managing the daily operations of the directorate in coordination with the other NGB Joint Staff directorates. These daily operations consist of Manpower & Personnel, Budget Planning, and Contracts Execution. The Deputy's focus on internal areas, allows the CIO/J6 Director to focus on the strategic direction of the directorate as well as senior-level engagement requirements across the DoD.

### **J63 - Joint C4 Operations Division**

The J63 (formally known as the C4 Division) has four branches. The Information Systems Branch, Information Management Branch, Joint C4 Coordination Center (JCCC), and Executive Communications Team (ECT). The J63, C4 Operations Division, provides C4/IT/communications support to the National Guard by enabling integrated IT capabilities for the National Guard JFHQ-S in support of the homeland security, homeland defense, and civil support missions. The J63 Division also provides deployable and interoperable communications technologies to the Army National Guard, Air National Guard, JFHQ-S, and its mission partners for use as a reliable and secure collaborative environment enabling interagency communications. Additionally, the J63 Division is responsible for the ECT that provides critical communications to the CNGB while outside of the National Capital Region (NCR).

### **J65 – Strategy and Policy Division**

The J65 (formally known as the CIO Division) has two branches. The Capabilities / Risk Management Framework Branch (RMF), and the IT Strategy & Governance Branch. The J65 Division focuses on internal and external IT governance and compliance. Additionally, the J65 provides expert advice and direct assistance to the CIO/J6, the NGB Joint Staff, and the CNGB. This includes strategic planning, oversight of strategic initiatives, and analysis of emerging IT capabilities to ensure the synchronized acquisition of IT resources.

## V. Deputy CIO/J6

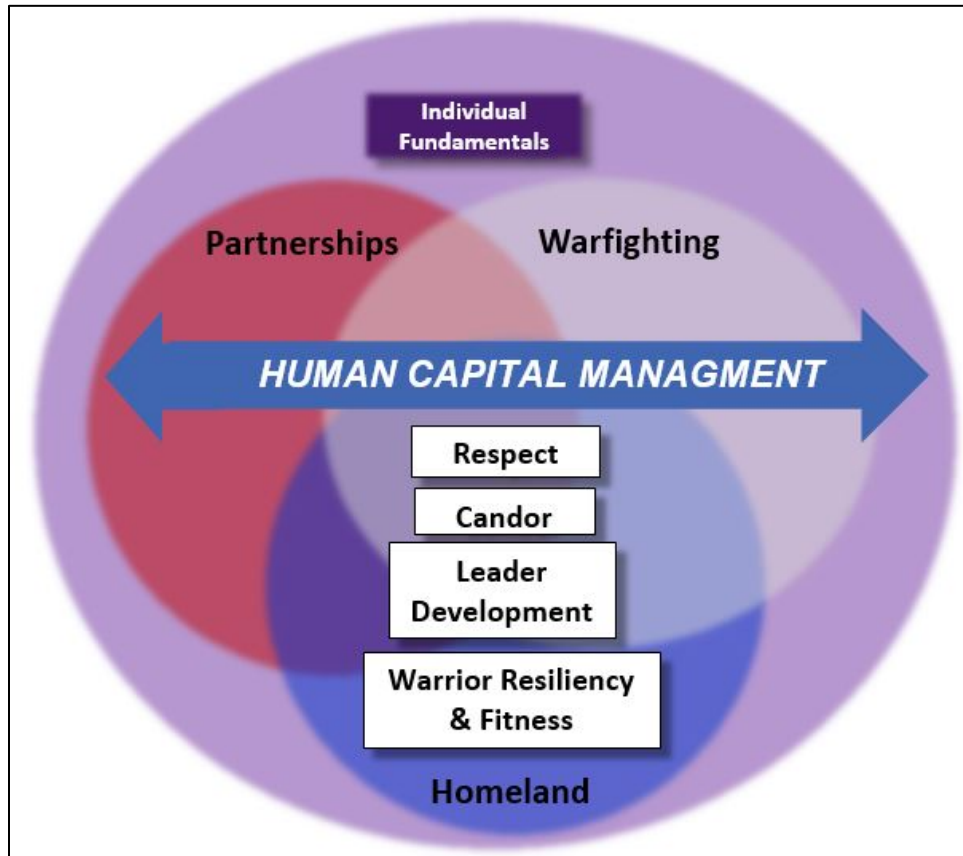


Figure 6 Human Capital Management

### Deputy CIO/J6 Key 500 Day Goals

#### 1. Human Capital Management

- a. Support the NGB CIO/J6 in managing the J6 team to excel. Support a positive command climate where all are respected and valued. Continue to grow as a team over the next 500 days and foster a productive and professional culture. As we grow our team, we will hire the right people with the right skills and the right attitude for us to excel. We will always treat our CIO/J6 personnel with dignity and respect, and challenge them to make the CIO/J6 and the NGB a better organization.
- b. Hire a NGB Chief Technology Officer (CTO) by Q3FY20.
- c. Hire a NGB Chief Data Officer (CDO) by Q4FY20.



- d. Validate the NGB IT budget that includes input from NGB Joint Staff, ARNG, and ANG NLT Q4FY20. The CIO/J6 will work in coordination with both the Army and Air National Guard to understand their IT capability needs and required resources. The goal is to ensure alignment to both NGB CIO/J6 and DoD CIO IT priorities while eliminating redundancies and leveraging successful IT initiatives in support of the National Guard.
- e. Fill 95% of the CIO/J6 positions by Q1FY21. Work aggressively to fill our vacant positions while reviewing and rewriting our CIO/J6 Position Descriptions for the talent and skillsets needed. An additional goal is to train hiring managers on the processes, timelines, and proper interview techniques to bring the best and brightest into the National Guard.
- f. Review, align, and manage our contract workforce for maximum synergy and effectiveness by Q1FY21. CIO/J6 must continually review our contract requirements and synchronize them with our CIO/J6 and NGB workforce requirements. Over the next 500 days, the staff will review contract requirements and deliverables to ensure we focus on priority tasks that support the NGB's priority missions.
- g. Execute 100% of CIO/J6 authorized budget.
- h. Align CIO/J6 with FY23-27 POM requirements in support of DoD and NGB IT reform initiatives.
- i. Establish a monthly NGB CIO/J6 forum with our ARNG G6 and ANG A2/3/6/10 partners to discuss current and future IT requirements and initiatives.

# VI. J63, C4 Operations Division

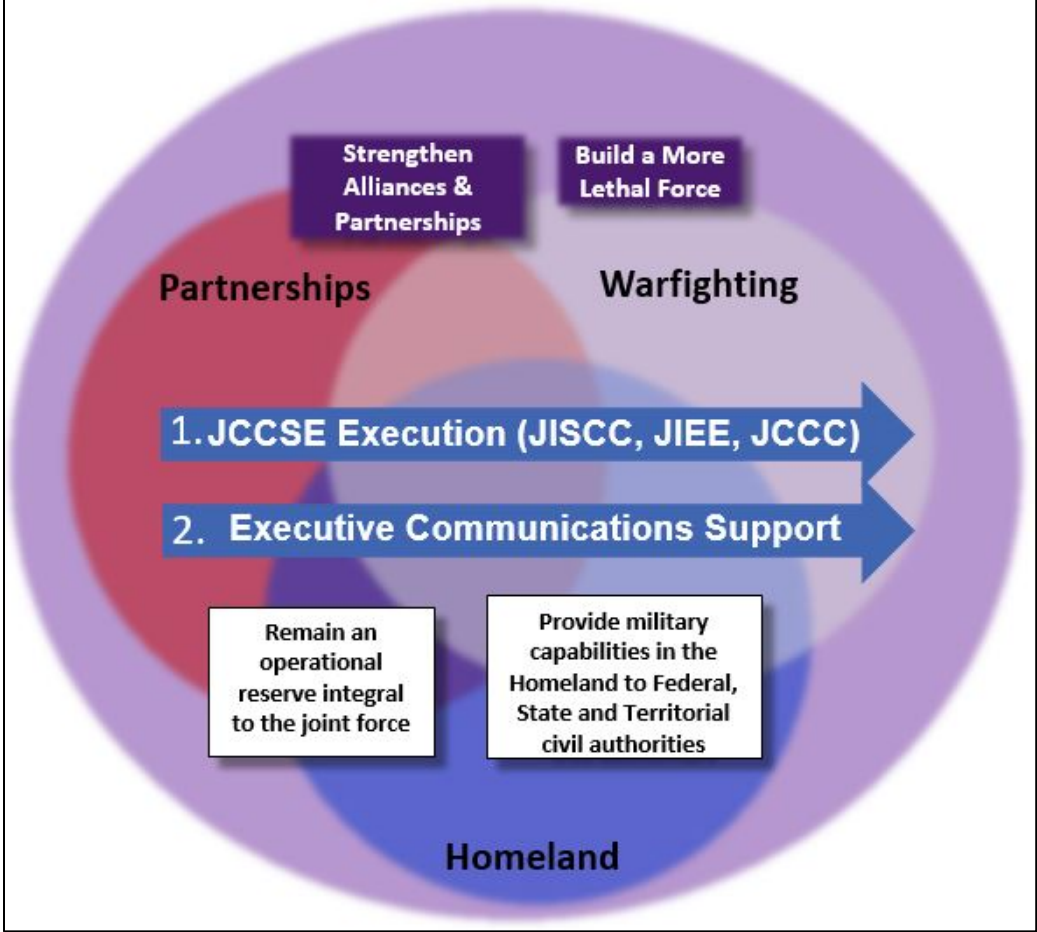


Figure 7: J63 LoEs

The J63 Division is directly responsible for two LoEs: *LoE 1 (JCCSE) (JISCC, JIEE, and JCCC)* and *LoE 2 Executive Communications Team Support*.

### J63 LoE 1. Core Functions

The Joint CONUS Communications Shared Environment (JCCSE) is an umbrella term that represents the flow of reliable and timely communications support to state and federal military activities, routine and otherwise, required for homeland defense, civil support, and other mission needs.

- Joint Incident Site Communication Capability (JISCC) – The J63 Division is the system owner for deployable commercial off the shelf (COTS) capability in support of DOMOPS.

- Joint Information Exchange Environment (JIEE) – The J63 Division is the system owner for JIEE, which is the NGB System of Record (SOR) for the dissemination of information, receiving, and processing Requests for Information (RFI), Requests for Assistance (RFA), personnel statistics, logistics statistics, and Commanders Critical Information Requirements (CCIRs).
- Joint Coordination Communication Center (JCCC) – The JCCC is the operational arm of the NGB CIO/J6. It assists in the design, planning, and employment of NGB communications assets in support of incident or natural disaster response communications requirements, participates in the planning and execution of national and regional DOMOPS exercises. It also coordinates with the JFHQ-S, Network Enterprise Center (NEC), Defense Information Systems Agency (DISA), Federal Emergency Management Agency (FEMA) and other partners to refine DOMOPS mission reporting requirements.

### **J63 LoE 2. Core Functions**

- Executive Communications Team (ECT) – The ECT provides critical communications to the CNGB while outside of the NCR including secure video, voice, and data, in support of CONUS and OCONUS missions. The team works closely with the J2 Technical Surveillance Counter Measure (TSCM) Team when planning and supporting the CNGB travel.

### **J63 Additional Responsibilities**

- Spectrum Management – Coordinate spectrum management support with combatant commands to conduct operations in congested and contested environments. Serves as part of the Joint Spectrum Management Element, planning and supporting spectrum management activities during domestic operations. Reviews spectrum policy, collaborates with the ARNG, ANG and other organizations in support of the spectrum programs throughout the 54 states and territories.
- Knowledge Management – Member of NGB Joint Staff core team to implement knowledge management for the NGB Joint Staff directorates. Administers J6 GKO SharePoint site. Facilitates the collection of NGB-J6 Lessons Learned observations during NG operations and exercises for input into the Joint Lessons Learned Information System. Participate in Lessons Learned Manager Working Group to review strategic observations requiring further actions to resolve.

# **J63 Key 500 Day Goals**

## **1. JCCSE Execution**

- a. Complete JISCC Block 2E (B2E) fielding NLT Q4FY20. The JISCC B2E effort serves to modernize the JISCC Block 2 and configure it to use commercial SATCOM. The New Equipment Training rotations are underway at this time. Complete initial rotations by Q3FY20. Schedule additional follow on rotations to complete the overall effort.
- b. Establish 60 DOMOPS C4 platforms on the NGB Commercial SATCOM Integrated Network (NGB-CSIN) NLT Q4FY20. Configuration of the JISCC B2Es and the Texas Interoperable Communications Package (TICPs) from the Texas National Guard to utilize NGB-CSIN. The CIO/J6, in coordination with select State National Guard IT communities, will establish some State-owned platforms on the NGB-CSIN as well. The goal is to provide satellite bandwidth for DOMOPS C4 platforms through a centrally funded and managed contract that allows for economies of scale and improved situational awareness.
- c. Begin JISCC Block 4 (B4) production NLT Q2FY21. Field the JISCC B4 capability so teams can meet the capability gap remaining once the fielding is complete for all the Disaster Incident Response Emergency Communication Terminal (DIRECT) systems. The JISCC B4 is currently undergoing requirements development. Naval Air Systems Command (NAVAIR) is designing a solution that supports B4 fielding by FY22.
- d. Complete a new JIEE operations and maintenance contract NLT Q4FY20. The current JIEE O&M contract expires 14 SEP 2020.
- e. Implement multi-factor authentication using Yubikey with JIEE NLT Q4FY20. This would allow emergency responders the ability to coordinate with their NG liaison officers and use JIEE to coordinate activities with JFHQ-S, State Emergency Management Authorities, and the National Guard Coordination Center (NGCC).
- f. Following the establishment of the Cloud Migration Plan, support the operational management, and sustainment of JIEE capability to the cloud.
- g. Develop and execute future JIEE acquisition strategy by Q2FY20. NGB CIO/J6 will work closely with the J3 team to identify and document current and future JIEE requirements. Once finalized we will work closely with the J8 and J3 to develop an acquisition strategy with multiple acquisition options to deliver the entire National Guard an Enterprise Information Exchange tool and environment. J63 will coordinate with J2, J3 and J8 to achieve a cloud-based initial operational capability (IOC) by Q3FY21.

- h. Implement the new SSA tool NLT Q3FY21. The CIO/J6 is pursuing multiple courses of action (COAs) for developing a future SSA tool that meets the National Guard's requirements. These efforts include engaging existing platforms while working on the acquisition process and coordinating with the Defense Innovation Unit.
- i. Develop and implement a JCCC cyber incident response framework for NGB.
- j. Establish operational procedures to plan, monitor, coordinate, track, and report the availability and usage of NGB-CISN NLT Q3FY20. By establishing its own commercial capability, NGB J6 will perform the tasks previously accomplished by DISA's Regional SATCOM Support Center (RSSC) and Contingency Exercise (CONEX) when utilizing Military Satellite (MILSAT). JCCC will test its procedures in the Q2FY20 communications exercise and will provide Joint Lessons Learned Information System (JLLIS) entries documenting any deficiencies.
- k. Improve communication flow between the CIO/J6, J65 liaison, and JCCC in support of NGCC and NGB J33 daily operations.
- l. Continue to improve JCCC response efforts and procedures to the NGCC during exercises and domestic operations.
- m. Compile Defense Readiness Reporting System (DRRS) reports to highlight shortfalls in the JFHQ-S J6's funding requests. Identify NGB CIO/J6 funding requests for the Joint Capability Assessment and Development Process (JCADP) for National Guard/Reserve Equipment Appropriation (NGREA) funding. This ensures the prioritization and packaging of communications appropriations for proper funding considerations.
- n. Lead NGB efforts to support the Joint Artificial Intelligence Center (JAIC) to include coordinating personnel to support the national mission initiatives. The responsibilities for this effort will eventually transition to the CTO.
- o. Coordinate NGB support to the Persistent Cyber Training Environment initiative ensuring an ATO is established and then transitioned to the J36 once operational.

## **2. Executive Communications**

- a. Establish Statement of Work with NAVAIR for program management of equipment solution NLT Q4FY20.
- b. Migrate ECT equipment to NGB-CSIN NLT Q4FY20.

## **3. Additional Responsibilities**

- a. Support electromagnetic spectrum operations during domestic operations including support for the Joint Electromagnetic Spectrum Operations Cell.

- b. Coordinate with JFHQ-S and the Services' Spectrum Management Office to activate the NG Interoperability Field Operations Guide (IFOG) in support of domestic operations.
- c. Shape DoD 5G strategy through the analysis and development of policies and procedures.
- d. Develop a knowledge management strategy by Q3FY20 to improve processes for knowledge flow, shared understanding, learning, and decision-making. Key to the development of the KM strategy will be identifying knowledge and performance gaps with immediate and long-term priorities based upon KM components that rely upon People, Processes, Tools, and Organizational concepts.

## VII. J65, Strategy and Policy Division

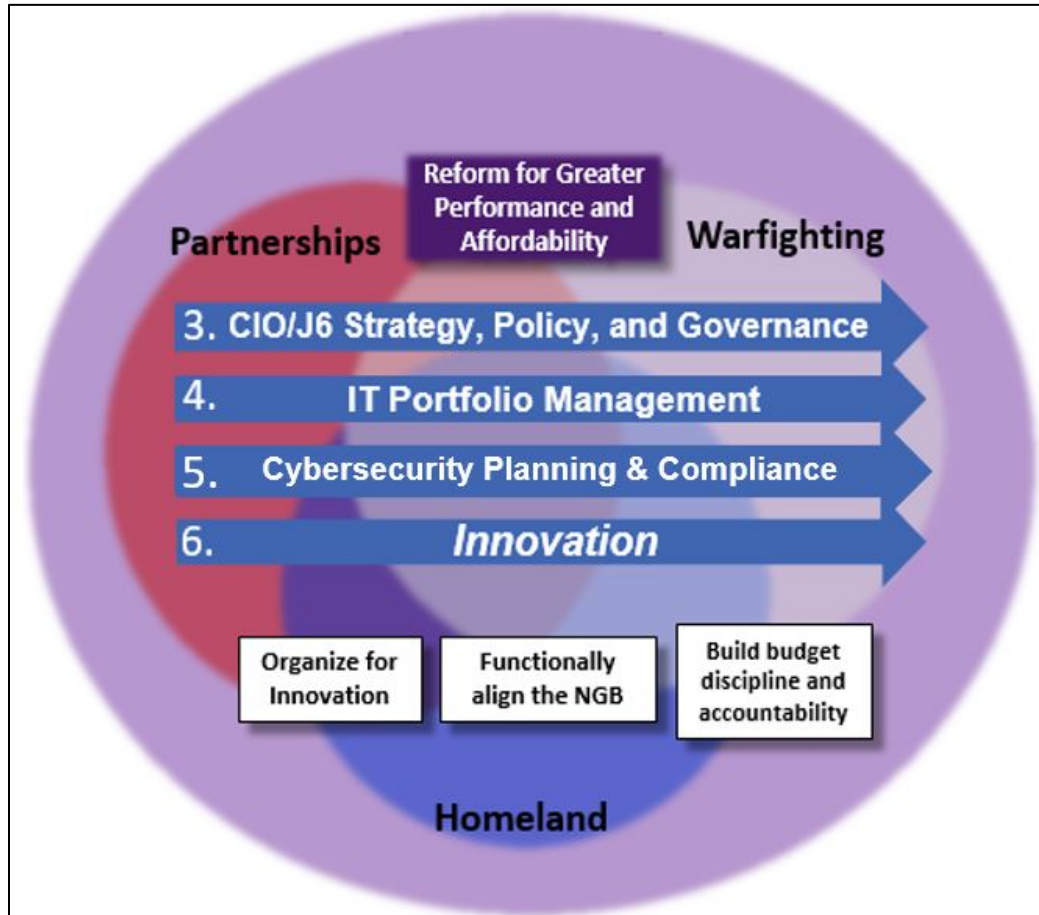


Figure 8: J65 LoEs

The J65 Division is directly responsible for four of the LoEs: *LoE 3 CIO/6 Strategy, Policy, and Governance*, *LoE 4 IT Portfolio Management*, *LoE 5 Cybersecurity Planning and Compliance*, and *LoE 6 Innovation*.

### J65 LoE 3 Core Functions

- IT Strategy and Governance – as the IT policy apparatus of the NGB, the J65 establishes near term and long term strategic plans as well as ensures compliance with DoD IT directives and governance.

### J65 LoE 4 Core Functions

- IT Portfolio Management – The systematic management of investments, projects and activities involving enterprise IT to include planned initiatives, projects, and ongoing IT services.

### **J65 LoE 5 Core Functions**

- Cybersecurity – The division ensures that systems/networks are compliant by mitigating vulnerabilities through the Risk Management Framework (RMF) process, the Command Cyber Readiness Inspection (CCRI) and Staff Assist Visits (SAV) in support of ATO requirements.

### **J65 LoE 6 Core Functions**

- Innovation – As one of the CNGB’s top priorities, innovation includes the consistent pursuit of ways to become more efficient, productive, and lethal. One current example of innovation is the Bring Your Own Device (BYOD) initiative aimed at increasing efficiency and ease of network access across the NG. New IT expanses that challenge the NG include Information Management (IM) that will provide Cloud Technology, Artificial Intelligence (AI) and Machine Learning (ML) technologies. The CNGB is dedicated to support the Joint Artificial Intelligence Center (JAIC) to include coordinating personnel to support the national mission initiatives of this newly established Department of Defense organization. While the J8 Directorate is the primary lead in the NGB for innovation, the CIO/J6 will work closely with the J8 and provide assistance as requested.

## **J65 Key 500 Day Goals**

### **1. CIO/J6 Strategy, Policy, and Governance**

- a. Develop a long term NGB IT 5-10 year Strategic Plan. This plan will be forward thinking and integrate IT initiatives from DoD, Army, Air Force, and partner ARNG and ANG organizations. It will guide us in properly fielding the latest IT technologies efficiently and effectively. IT is a critical enabler and requires forward-thinking, planning, and synchronized execution. It will make our force more lethal and capable while wisely expending our limited IT budgets. The primary objective of this plan is to develop and recommend to the NGB CIO/J6 Senior Leadership a 5-10 year strategic plan that outlines where the NG should be in the future. This future state would garner IT efficiencies, enhance interoperability, improve geospatial information sharing, and increase mission effectiveness between the NGB, the 54 JFHQ-S, and our mission partners.
- b. Manage the CIO Executive Council (CEC). The J65 will continue to manage the CEC using it as both an information forum and decision body for NGB wide IT initiatives. The goal is to conduct a minimum of two 06/GS15 level meetings and two flag officer/SES



level sessions annually. The CIO/J6 briefs the CNGB after each flag officer session. The goal is to continue maturing this governing process over the next 500 days into the NGB forum for IT-related information updates and decisions.

- c. Establish a monthly NGB CIO/J6 Synchronization Board with our ARNG G6 and ANG A2/3/6/10 partners to discuss and synchronize current and future IT requirements and initiatives. The CIO/J6 staff also participates in many DoD level IT forums to ensure representation of NG equities. By leveraging these relationships, the NGB CIO/J6 will maintain good rapport with the DoD CIO, and the leadership of the Army G6 and Air Force ANG A2/3/6/10.
- d. Maintain and sustain full partnership in the DoD Mission Partner Environment (MPE) forums to ensure National Guard equities are fully considered and included in MPE planning and execution. MPE applies to a broad spectrum of missions including, but not limited to, Major Combat Operations (MCO), Humanitarian Assistance and Disaster Relief (HA/DR), Military Force Assistance and Stability Operations, Joint All Domain Command and Control (JADC2) and Defense Support of Civil Authorities (DSCA). MPE is flexible and scalable to accommodate all levels of warfare (strategic, operational, or tactical). Selective Cross-Domain Services (CDS) voice, video, chat, and email services will be required to ensure access and information flow between security domains.

## **2. IT Portfolio Management**

- a. Manage IT Investment Reviews (Annually). The J65 CIO team will work with each directorate to review all IT investments on an annual basis after approval of the Resource Validation Board (RVB). The goal for this activity over the next 500 days is to ensure that beginning in FY21 the CIO/J6 will have set the conditions to include NGREA and Program Objective Memorandum (POM) IT requirements. This will synchronize NGB IT investments and provide for transparent IT budget execution. NGB J65 team will work closely with the NGB Joint Staff, ARNG G6, and ANG A2/3/6/10 to review NGB IT investments. This process will also help the CIO/J6 align IT efforts with the DoD, Army, and Air Force CIO communities.
- b. Manage NGB Joint Service Provider (JSP) Migration for IT reform and efficiency. During Q2FY20 the NGB primary staff in the Pentagon will transition to JSP provided IT services from their current DoD Information Networks (DoDIN-A) service. The IT services provided include Non-Secure Internet Protocol Routing (NIPR), Secure Internet Protocol Routing (SIPR), Phone, Video, and Cellphone services.
- c. Synchronize CIO/J6 future contract efforts in partnership with the J63 and the CIO/J6 Deputy. The team will review current and future contract requirements and modify them as required to maximize the synergy in support of the NGB mission requirements.

- d. Develop and implement a NGB Cloud Migration Plan as part of the DoD strategy. Continue analyzing and assessing cloud migration services including Joint Enterprise Defense Infrastructure (JEDI), milCloud, and other Commercial/Government-Cloud alternatives for viability across the National Guard. The J65 will work with NGB, ARNG, ANG, and the 54 to identify and prioritize opportunities for accelerating cloud adoption. The ongoing goal for this initiative is to continue coordinating with the NGB Joint Staff investments to plan and execute cloud migration activities. The J65 is developing cloud migration outreach services to assist the 54 with identifying, planning, and executing cloud migration as appropriate.
- e. Leverage DoD Enterprise contract initiatives such as Joint Enterprise Defense Infrastructure (JEDI), Enterprise Collaborations and Productivity Services (ECAPS) and Defense Enterprise Office Solution (DEOS) across the entire National Guard to include ARNG G-6 and ANG A2/3/6/10 initiatives. The goal is to ensure that the CIO/J6 capitalizes on efficient contract vehicles to deliver effective enterprise IT capabilities across the National Guard.
- f. Work in cooperation with J3 and J8 to facilitate an SSA Working group to field a future SSA capability NLT Q3FY21. The working group will identify, prioritize, and implement doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF) recommendations for SSA gap closure. J65 has developed an initial capability requirements document (CRD) that CIO/J6 will utilize for acquiring modernized capabilities in support of SSA information sharing between NGB, the 54, NORTHCOM, and all other mission partners.

### **3. Cybersecurity Planning and Compliance**

- a. Continue to develop NGB RMF/CCRI/SAV in support of the Cybersecurity framework to ensure 100% compliance with DoD regulatory guidance. The goal for this activity over the next 500 days is to develop a synchronized NGB RMF/ CCRI/ Staff Assist Visit (SAV), inspection and remediation program as part of the NGB Cybersecurity Manual. J65 will fully support the CIO/J6 in his role as Authorizing Official (AO) to accredit key NG IT systems.

### **4. Innovation**

- a. Identify and align NGB technology requirements in synchronization with the DoD CIO, Army, and Air Force communications communities. The CTO will closely align with the

newly hired CDO to develop NGB's data and technical frameworks to leverage both AI and ML.

- b. Establish a data management framework throughout the entire National Guard in FY21. The CDO will help the National Guard understand where our data resides across our environment and how to implement a governance structure using the innovative technologies of AI and ML capabilities in support of senior leader decision making.
- c. Participate in DISN's and ARNG G6's BYOD initiatives in Q3FY20. The J6 and ARNG G6 are collaborating to examine the possibilities for establishing BYOD capabilities in the National Guard. Leveraging this BYOD capability will provide NG members with greater ease of network access and online resources. It will also significantly assist NG Soldiers and Airman with obtaining access to .mil resources on personnel devices.

## VIII. Closing Remarks

The NGB CIO/J6 Directorate is committed to the mission of supporting the homeland and winning future wars abroad. Every Soldier and Airman across our National Guard IT community is vital to the success of the team.

This 500-Day Plan serves as the basis for the 500-Day Implementation Plan and the long term 5 to 10-year strategic plan development. It guides our NGB CIO/J6 Directorate leaders and workforce in making informed decisions.

We will continue to grow as a team over the next 500 days and foster a positive climate and professional culture to execute key NGB CIO/J6 IT initiatives. This is a challenging time, but also an exciting time to serve in the National Guard IT community. I believe this 500-Day Plan will guide us to meet the challenges of tomorrow.

As we meet the challenges, supporting both our non-Federal and Federal requirements, we will rise to the occasion. Using this 500-Day IT plan as a guide, the NG will continue on its transformational journey through innovation and increased readiness so that when it's time to answer the nation's call, the NG will stand ready.



## Appendix A. References

1. Army National Guard Vision and Strategy 2017
2. DoD CIO Capability Programming Guidance FY 2022-2026
3. DoD Digital Modernization Strategy July 12, 2019
4. DoD Directive 51011.77 30 October 2015
5. National Defense Strategy 2018
6. National Guard Bureau Posture Statement 2019
7. National Guard National Defense Strategy Implementation Guidance
8. National Military Strategy 2018
9. National Security Strategy December 2017
10. Joint Doctrine Note 2-19 10 December 2019

## Appendix B. Acronyms

<b>Acronym</b>	<b>Definition</b>
AI	Artificial Intelligence
ANG	Air National Guard
ARCYBER	Army Cyber Command
ARNG	Army National Guard
ASAP	as soon as possible
ATO	Authority To Operate
BYOD	Bring Your Own Device
CCB	Configuration Control Board
CCRI	Command Cyber Readiness Inspection
CDO	Chief Data Officer
CDS	Selective Cross-Domain Services
CEC	Chief Executive Council
CIO	Chief Information Officer
CNGB	Chief of the National Guard Bureau
CONUS	Continental United States
COP	Common Operational Picture
CONEX	Contingency Exercise
COTS	Commercial Off The Shelf
CPIC	Capital Planning and Investment Control
CRD	Capability Requirements Document
CS	Cybersecurity
CSIN	Commercial SATCOM Integrated Network
CTO	Chief Technical Officer
DA	Department of the Army
DAART	Domestic Operations Awareness and Assessment Response Tool
DAF	Department of the Air Force
DCIO	Department of Defense Chief Information Officer
DEOS	Defense Enterprise Office Solution
DIRECT	Disaster Incident Response Emergency Communication Terminal
DISA	Defense Information Systems Agency
DSCA	Defense Support of Civil Authorities
DOIM	Directorate Of Information Management
DoDIN	Department of Defense Information Networks
DOMOPS	Domestic Operations
DOTMLPF	Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, and Facilities
DRRS	Defense Readiness Reporting System

ECAPS	Enterprise Collaborations and Productivity Services
ECT	Executive Communications Team
FEMA	Federal Emergency Management Agency
FY	Fiscal Year
IFOG	Interoperability Field Operations Guide
IM	Information Management
HA/DR	Humanitarian Assistance and Disaster Relief
IOC	Initial Operational Capability
IT	Information Technology
JADC2	Joint All Domain Command and Control
JAIC	Joint Artificial Intelligence Center
JCADP	Joint Capability Assessment and Development Process
JCCC	Joint Communications Control Center
JCCSE	Joint CONUS Communications Shared Environment
JEDI	Joint Enterprise Defense Infrastructure
JFHQ	Joint Force Headquarters
JIE	Joint Information Environment
JIEE	Joint Information Exchange Environment
JLLIS	Joint Lessons Learned Information System
JISCC	Joint Incident Site Communications Capability
JS	Joint Staff
JSP	Joint Service Provider
LoE	Line of Effort
MILDEP	Military Department
MILSAT	Military Satellite
ML	Machine Learning
MPE	Mission Partner Environment
NAVAIR	Naval Air Systems Command
NCR	National Capital Region
NDS	National Defense Strategy
NG	National Guard
NGB	National Guard Bureau
NGCC	National Guard Coordination Center
NGBSP	National Guard Bureau Strategic Plan
NGREA	National Guard/Reserve Equipment Appropriation
NGSE	National Guard Strategic Estimate
NIPR	Non Secure Internet Protocol Routing
NLT	No Later Than
NMS	National Military Strategy

NORTHCOM	United States Northern Command
NSS	National Security Strategy
OCONUS	Outside Continental United States
POM	Program Objective Memorandum
PPBE	Planning Programming and Budget Execution
RFA	Request for Assistance
RFI	Request for Information
RMF	Risk Management Framework
RSSC	Regional SATCOM Support Center
RVB	Resource Validation Board
SATCOM	Satellite Communications
SAV	Staff Assist Visit
SES	Senior Executive Service
SIPR	Secret Internet Protocol Routing
SSA	Shared Situational Awareness
SOR	System Of Record
TICP	Texas Interoperable Communications Package
TSCM	Technical Surveillance Counter Measure
USCYBERCOM	United States Cyber Command



## Appendix C. NGB CIO/J6 Directorate Key 500 Day Goals

Goal Statement	Ref Pg.
1. NGB CIO/J6 Directorate will continue to grow as a team over the next 500 days and foster a positive climate and professional culture.	11 – 1a
2. Hire a NGB Chief Technology Officer (CTO) by Q3FY20.	11 – 1b
3. Hire a NGB Chief Data Officer (CDO) by Q4FY20.	11 – 1c
4. Validate the NGB IT budget that includes input from NGB Joint Staff, ARNG, and ANG NLT Q4FY20.	12 – 1d
5. Fill 95% of the CIO/J6 positions by Q1FY21.	12 – 1e
6. Review, align, and manage our contract workforce for maximum synergy and effectiveness by Q1FY21.	12 – 1f
7. Execute 100% of CIO/J6 authorized budget.	12 – 1g
8. Align CIO/J6 with FY23-27 POM requirements in support of DoD and NGB IT reform initiatives.	12 – 1h
9. Establish a Monthly NGB CIO/J6 Forum with our ARNG G6 and ANG A2/3/6/10 partners to discuss current and future IT requirements and initiatives.	12 – 1i
10. Complete JISCC Block 2E (B2E) fielding NLT Q4FY20.	15 – 1a
11. Establish 60 DOMOPS C4 platforms on the NGB Commercial SATCOM Integrated Network (NGB-CSIN) NLT Q4FY20.	15 – 1b
12. Begin JISCC Block 4 (B4) production NLT Q2FY21.	15 – 1c
13. Complete a new JIEE operations and maintenance contract NLT Q4FY20.	15 – 1d
14. Implement multi-factor authentication using Yubikey with JIEE NLT Q4FY20.	15 – 1e
15. Following the establishment of the Cloud Migration Plan, support the operational management, and sustainment of JIEE capability to the cloud.	15 – 1f
16. Develop and execute future JIEE acquisition strategy by Q2FY20.	15 – 1g
17. Implement the new SSA tool NLT Q3FY21.	16 – 1h
18. Develop and implement a JCCC cyber incident response framework for NGB.	16 – 1i
19. Establish operational procedures to plan, monitor, coordinate, track, and report the availability and usage of NGB-CISN NLT Q3FY20.	16 – 1j
20. Improve communication flow between the CIO/J6, J65 liaison, and JCCC in support of NGCC and NGB J33 daily operations.	16 – 1k
21. Continue to improve JCCC response efforts and procedures to the NGCC during exercises and domestic operations.	16 – 1l
22. Compile Defense Readiness Reporting System (DRRS) reports.	16 – 1m
23. Lead NGB efforts to integrate with the Joint Artificial Intelligence Center (JAIC).	16 – 1n
Goal Statement	Ref Pg.

24. Coordinate NGB support to the Persistent Cyber Training Environment initiative ensuring an ATO is established and then transitioned to the J36 once operational.	16 – 1o
25. Establish Statement of Work with NAVAIR for program management of equipment solution NLT Q4FY20.	16 – 2a
26. Migrate ECT equipment to NGB-CSIN NLT Q4FY20.	16 – 2b
27. Support electromagnetic spectrum operations during domestic operations including support for the Joint Electromagnetic Spectrum Operations Cell.	16 – 3a
28. Coordinate with JFHQ-S and the Services' Spectrum Management Office to activate the NG Interoperability Field Operations Guide (IFOG) in support of domestic operations.	17 – 3b
29. Shape DoD 5G strategy through the analysis and development of policies and procedures.	17 – 3c
30. Develop a knowledge management strategy by Q3FY20.	17 – 3d
31. Develop a long term NGB IT 5-10 year Strategic Plan.	19 – 1a
32. Manage the CIO Executive Council (CEC).	19 – 1b
33. Establish a monthly NGB CIO/J6 Synchronization Board with our ARNG G6 and ANG A2/3/6/10 partners.	20 – 1c
34. Maintain and sustain full partnership in the DoD Mission Partner Environment (MPE) forums.	20 – 1d
35. Manage IT Investment Reviews (Annually).	20 – 2a
36. Manage NGB Joint Service Provider (JSP) Migration for IT reform and efficiency.	20 – 2b
37. Synchronize CIO/J6 future contract efforts.	20 – 2c
38. Develop and implement a NGB Cloud Migration Plan as part of the DoD strategy.	21 – 2d
39. Leverage DoD Enterprise contract initiatives across the entire National Guard.	21 – 2e
40. Work in cooperation with J3 and J8 to facilitate an SSA Working group to field a future SSA capability NLT Q3FY21.	21 – 2f
41. Continue to develop NGB RMF/CCRI/SAV in support of the Cybersecurity framework to ensure 100% compliance with DoD regulatory guidance.	21 – 3a
42. Identify and align NGB technology requirements in synchronization with the DoD CIO, Army, and Air Force communications communities.	21 – 4a
43. Establish a data management framework throughout the entire National Guard by FY21.	22 – 4b
44. Participate in DISN's and ARNG G6's BYOD initiatives in Q3FY20.	22 – 4c

