



UNITED STATES CYBER COMMAND
9800 SAVAGE ROAD, SUITE 6171
FORT GEORGE G. MEADE, MARYLAND 20755

Re: 21-R038

Mark Pomerleau



JUN 27 2025

Dear Mr. Pomerleau,

This letter responds to the enclosed Freedom of Information Act (FOIA) request, submitted to U.S. Cyber Command on April 5, 2021. We clarified the scope of your request with you on April 15, 2021, via email.

We have located and reviewed 19 pages of material responsive to your request. As the Initial Denial Authority, I have determined that the redacted information is exempt from disclosure under the FOIA, title 5, United States Code, section 552(b)(1), (b)(3), (b)(5), and (b)(6). Details of the specific exemptions cited are attached to this letter.

If you are not satisfied with our action on this request, you may seek dispute resolution services from the Department of Defense (DoD) FOIA Public Liaison or the Office of Government Information Services. You also have the right to file an administrative appeal. Contact information for each resource is enclosed.

KENNETH J. BURGESS
Brigadier General, U.S. Army
Acting Chief of Staff

Enclosures:
a/s

JUN 27 2025

Re: 21-R038

FOIA Exemptions Cited:*

(b)(1) – information properly and currently classified in the interest of national defense or foreign policy, pursuant to Executive Order 13526, Classified National Security Information;

Section 1.4(a) – military plans, weapons systems, or operations;

Section 1.4(g) – vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security.

(b)(3) – information specifically exempted from disclosure by statute:

10 U.S.C. §130b, personally identifying information of DoD personnel in sensitive units;

10 U.S.C. §130e, defense critical infrastructure security information.

(b)(5) – inter- or intra-agency memoranda containing information that qualifies for deliberative process privilege.

(b)(6) – information in personnel and medical files and similar files, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.

* The FOIA provides that a federal agency or department may withhold responsive records only if: (1) the agency reasonably foresees that disclosure would harm an interest protected by one of the nine exemptions; or (2) disclosure is prohibited by law. 5 U.S.C. §552(a)(8)(A)(i). Note that we have considered the foreseeable harm standard when reviewing the records and applying FOIA exemptions. This standard is used to determine whether information may be disclosed even if it technically falls within an exemption.

DoD FOIA Public Liaison:

Ms. Virginia Burke
Phone: (571) 371-0462
Email: osd.mc-alex.oatsd-pclt.mbx.foia-liaison@mail.mil

Office of Government Information Services:

Office of Government Information Services
National Archives and Records Administration
8601 Adelphi Road – OGIS
College Park, MD 20740-6001
Email: ogis@nara.gov
Phone: (202) 741-5770
Toll Free: 1-877-684-6448
Fax: (202) 741-5769

Administrative Appeal:**

Ms. Joo Chung
Assistant to the Secretary of Defense for Privacy, Civil Liberties, and Transparency (PCLT)
Office of the Secretary of Defense
4800 Mark Center Drive
ATTN: PCLFD, FOIA Appeals
Mailbox #24
Alexandria, VA 22350-1700
Email: osd.foia-appeal@mail.mil

** Appeal should cite case number above, be clearly marked "FOIA Appeal" and filed within 90 calendar days from the date of this letter.

FOIA Request 207906

The following list contains the entire submission submitted April 05, 2021 02:30:02pm ET, and is formatted for ease of viewing and printing.

Contact information

First name	Mark
Last name	Pomerleau
Mailing Address	<div></div>
City	
State/Province	
Postal Code	
Country	
Phone	
Company/Organization	
Email	

Request

Request ID	207906
Confirmation ID	207381
Request description	I request records and documents related to the creation of U.S. Cyber Command's Capability Development Group (CDG), CDG's missions and activities, and the CDG's dissolution into the J9.

Supporting documentation

Additional Information	Mark Pomerleau Freedom of Information Act Request -- U.S. Cyber Command Capabilities Development Group.docx
-------------------------------	---

Fees

Request category ID	media
Fee waiver	yes
Explanation	I am requesting a fee waiver as I am a media member and these records are being sought for non-commercial purposes and will serve to greater inform the American public about urgent and vital issues of widespread national interest.

Expedited processing

Expedited Processing

no

USCYBERCOM/J0 FOIA
9800 Savage Road STE 6171
Fort George G. Meade, MD 20755

Telephone: [redacted]
FAX: (443) 654-4778
Electronic Mail: TBD

USCYBERCOM/J0 FOIA
9800 Savage Road STE 6171
Fort George G. Meade, MD 20755

Dear FOIA Officer,

Under the Freedom of Information Act (5 U.S.C. 552), I request all documents from Jan. 1, 2012 to present related whole or in part to:

- o The creation of the Capabilities Development Group (CDG)
- o The CDG's roles, goals and missions
- o The CDG's yearly budget for each year it existed
- o The number of personnel assigned to CDG for each year it existed as well as names, titles and job descriptions of such personnel
- o Oversight of requirements CDG issued for capabilities
- o Internal projects CDG worked on in house without outsourcing such as quick reaction capabilities or urgent needs capabilities
- o CDG support to Joint Task Force Ares
- o Dissolution of CDG and reabsorption back into the J9
- o J9's roles, goals and missions as they relate to requirements and capability development since the CDG was reabsorbed
- o The J9's budget as it applies to capability development and requirements since the CDG was reabsorbed

21-R038

withdrawn

I request electronic copies of documents including, but not limited to, memos, emails, correspondence, execute orders, PowerPoint presentations, status reports and/or reports.

In order to help you determine my status you should know that I am a representative of the news media affiliated with C4ISRNET and Defense News, and this request is made as part of news gathering and not for commercial use.

I also request a fee waiver as I am a media member and these records are being sought for non-commercial purposes and will serve to greater inform the American public about urgent and vital issues of widespread national interest.

My preference is to receive corresponding records in an electronic format via email to

[redacted]

If you choose to deny this request, please provide a written explanation for the denial including a reference to the specific statutory exemption(s) upon which you rely. Also, please provide all segregable portions of otherwise exempt material, as required.

Please contact me at [redacted] and [redacted] if I can clarify or expedite this request.

Thanks in advance,

Sincerely,

Mark Pomerleau





DEPARTMENT OF DEFENSE
UNITED STATES CYBER COMMAND
9800 SAVAGE ROAD, SUITE 6171
FORT GEORGE G. MEADE, MARYLAND 20755

FEB 16 2016

Reply to:
Commander

MEMORANDUM FOR THE JOINT DIRECTORS, SPECIAL STAFF, COMMANDER,
CYBER NATIONAL MISSION FORCES

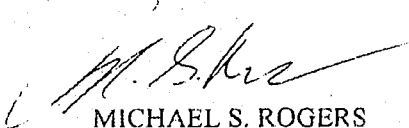
SUBJECT: Establishment of the United States Cyber Command Capabilities Development Group (CDG)

1. This memorandum establishes the Capabilities Development Group (CDG) as a distinct and core element of the U.S. Cyber Command staff. The CDG is directed to coordinate, integrate, and prioritize cyberspace capability development efforts to rapidly deliver joint operational products through integrated project delivery, enabling full-spectrum cyberspace operations. Specifically, the CDG Director shall:

- Translate operational needs to capability requirements, identify gaps between them, and develop the activities and plans to address capability gaps.
- Coordinate, prioritize, and enable capability development across the USCYBERCOM directorates and supporting organizations.
- Rapidly procure and/or deliver joint products with associated sustainment plans to meet current and future mission needs.

2. The CDG is established at initial operating capability (IOC) with [redacted] as the Director, [redacted] as the Deputy Director, and [redacted] as the Executive Director. The CDG will incorporate the J3 Special Projects Team and the J6 and J9 directorates, and be responsible for the associated missions. CIO support and SAE responsibilities will reside within the CDG. This memorandum further directs an FOC plan to be completed no later than 90 days from the date of signature. The FOC plan will detail additional functions and roles to be assumed by the CDG.

3. The POC for this action is [redacted]


MICHAEL S. ROGERS
Admiral, U.S. Navy
Commander



TOP SECRET // NOFORN



(U) INFORMATION PAPER

(b) (3) 10 U.S.C. §130e

(U) CDG Overview

(U) **Purpose:** Provide an overview of the Capability Development Group (CDG) mission, goals, major responsibilities, and

(U) **CDG Mission and Goals:** The *mission* of the CDG is to plan, synchronize, and execute joint capability development and services to enable USCYBERCOM to execute its mission. In order to achieve this mission, the CDG works under two *goals*:

- (U//FOUO) Establish [redacted] to enable combined arms, offensive operations, and defensive operations.
- (U) Meet current operational needs of the Cyber Mission Force (CMF).

(U//FOUO) **CDG Responsibilities:** Having been established in February 2016, the CDG provides the centralized effort for capability development in partnership with the Service Cyber Components (SCCs) and greater community of developers. It also exercises a limited acquisition authority under the CDG's Command Acquisition Executive (CAE) for the acquisition, development, and sustainment of Cyber Operations-peculiar equipment and capabilities (FY16 Nat'l Defense Authorization Act, Sec. 807). This authority is capped at \$75M annually and will expire at the end of FY20 unless modified by Congress. Additionally, the Director, CDG serves as the Chief Information Officer for the Command. The

(U) **CDG Objectives:** Having built its foundation, the CDG is now working toward its steady state *vision* of "unprecedented capability delivery for the CMF." In fiscal year 2018 (FY18) the CDG is operating to achieve six *objectives*:

1. (U) Deliver capabilities against high priority cyber needs requested by our operational partners in accordance with the FY18 Capability Development Plan.
2. (U) Complete CDG build-out by recruiting and retaining world-class talent consistent with CDG core values (excellence, teamwork, effective communications).
3. (U) Fully utilize current acquisition authority while establishing relevant acquisition policies and growing staff to meet expanded authorities at USCYBERCOM elevation.
4. (U) Grow CDG's teamwork, visibility, and credibility with Service Cyber Component partners to enhance joint capability outcomes.
5. (U) Strengthen our access and interactions with community cyber S&T partners to influence their resource investments to benefit Command priorities.
6. (U) Define and implement a comprehensive risk management process for the Command's Cyberspace Mission Systems, HQ Business Systems, and Developmental Systems / Environments.

(U) CDG Highlights:

- (TS//NF) [redacted]
- (TS//NF) [redacted]
- (U//FOUO) [redacted]

(b) (3) 10 U.S.C. §130e

Classified By: [redacted]
Derived From: USCYBERCOM SCG
Dated: 2016015
Declassify On: 20440420

(b) (1) Sec. 1.4 (a) (g)

TOP SECRET // NOFORN

(b) (3) 10 U.S.C. §130b

(b) (6)

~~TOP SECRET // NOFORN~~

- (U//~~FOUO~~) *Acquisition delivery*: CDG awarded a contract to provide information technology services to embedded foreign partner personnel. As part of a USCYBERCOM objective, this effort will allow improved staff integration and foreign partner cooperation.
- (U//~~FOUO~~) *Technical Outreach*: CDG held the second Cyber Capability Update Conference with the SCC development organizations to form a common understanding of development roles and vision for [REDACTED]

(U) Candidate FY19 CDG Objectives:

1. (U//~~FOUO~~) Continue to recruit, retain and sustain world-class talent to ensure development and delivery of needed cyber capabilities for the CMF.
2. (U//~~FOUO~~) In collaboration with the Service Cyber Components, achieve a common understanding of [REDACTED] for accepted standards, interfaces, protocols, and scope.
3. (U//~~FOUO~~) Grow RASA capacity to accelerate solution development and capability delivery to the CMF.
4. (U//~~FOUO~~) Generate and maintain a cyber operational capability inventory on behalf of the Command
5. (U//~~FOUO~~) Employ acquisition processes to satisfy CMF requirements using the full range of tools consistent with available authorities
6. (U//~~FOUO~~) Posture the USCYBERCOM Developer Community (to include the Service Cyber Components) to enable rapid cyber capability delivery.

(U//~~FOUO~~) [REDACTED]
[REDACTED]

(U//~~FOUO~~) [REDACTED]
[REDACTED]

(U//~~FOUO~~) [REDACTED]
[REDACTED]

(U//~~FOUO~~) [REDACTED]
[REDACTED]

(U) Date of Material:
(U) Originator:
(U) Classification Review By:

~~TOP SECRET // NOFORN~~

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

USCYBERCOM CAPABILITIES DEVELOPMENT GROUP IMPLEMENTATION PLAN

CAPABILITIES DEVELOPMENT GROUP

16 May 2016



UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

Table of Contents

1 (U) Background.....	1
2 (U) Mission and Functions.....	1
(U) CDG Mission	1
(U) Guiding Principles.....	1
(U) Major Functions.....	2
3 (U) Mission Execution	2
4 (U) Organizational Structure	7
(U) Front Office Personnel / Chief Information Officer / Command	
Acquisition Executive	8
(U) Technical Outreach	9
(U) CDG/J6 - Operational Architecture & C4 Systems and CIO Support	
Directorate.....	10
(U) Applied Research & Development.....	11
(U) Mission Integration.....	12
(U) Acquisition.....	13
5 (U) Implementation	14
6 (U) Plan Approval	14

1 (U) Background

(U//~~FOUO~~) The Capabilities Development Group (CDG) was instituted by the Commander of United States Cyber Command (USCYBERCOM) on February 16, 2016 as a distinct and core element of the USCYBERCOM staff. The CDG was directed to coordinate, integrate, and prioritize cyberspace capability development efforts to rapidly deliver joint operational products through integrated project delivery, enabling full-spectrum cyberspace operations. The CDG Director was charged with:

- Translating operational needs to capability requirements, identifying gaps between them, and developing the activities and plans to address capability gaps.
- Coordinating, prioritizing, and enabling capability development across the USCYBERCOM directorates and supporting organizations.
- Rapidly procuring and/or delivering joint products with associated sustainment plans to meet current and future mission needs.

(U//~~FOUO~~) The CDG was established at Initial Operating Capability (IOC) on February 16, 2016 with a Director, Deputy Director, and Executive Director. Additionally, J3 Special Projects and the J6 and J9 Directorates were incorporated into the CDG. In the CDG establishment memo, the Commander, USCYBERCOM directed that a full operational capability (FOC) plan be completed by May 16, 2016. This implementation plan is submitted to fulfill that requirement. This plan outlines the functions and structure the CDG will assume upon approval.

2 (U) Mission and Functions

(U) CDG Mission

(U//~~FOUO~~) In accordance with the Commander's establishment memo, the mission of the CDG is as follows:

The CDG plans and synchronizes joint capability development for the cyberspace domain, rapidly delivers mission-ready operational products and services required for generating, facilitating, or monitoring effects, and operates and maintains USCYBERCOM's technical baseline to enable the Command to execute its missions.

(U) Guiding Principles

(U//~~FOUO~~) The CDG will seek to deliver mission-ready capabilities that are ready to be used by the Cyber Mission Forces and include all factors necessary to execute the given mission. The guiding principles for the CDG are to foster and maintain strong teamwork, cross-capability integration, technical acumen, and acquisition expertise. Capability development will be conducted as a team effort within the Command, the Department of Defense, and other partners such as academia, industry, and government sponsored laboratories. The CDG will build strong teams with the Services and other partners to contribute to and manage mission-ready capabilities that enable command and execution of integrated cyber operations. Additionally,

integration is inherent to the CDG mission. The CDG will seek to integrate different capabilities into a single operational architecture to enable defensive and offensive missions. The CDG will unify existing and evolving technology in support of integrated full spectrum cyber operations by defining and enforcing interoperability standards for acquisition and development.

(U) Major Functions

(U//~~FOUO~~) The major functions of the CDG include:

- Create and maintain the Command's operational architecture, as authorized.
- Build and manage the plan to realize mission-ready capabilities defined in the architecture by evaluating priorities from a technical and operational perspective.
- Develop capabilities through partnership across the Command, Service Cyber Components, Services/Agencies, mission partners, industry, and others.
- Define, maintain, and enforce technical standards to ensure integration, as authorized.
- Support transition of capabilities to operational forces.
- Define, build, and maintain the technical baseline for the Command.
- Execute Chief Information Officer (CIO) responsibilities.
- Execute Command Acquisition Executive (CAE) responsibilities, when authorized.

3 (U) Mission Execution

(U//~~FOUO~~) In accordance with the CDG guiding principles, teaming is required for capabilities to be integrated and mission ready. Teaming will be accomplished primarily through Integrated Products Teams (IPTs), which will require participation from across the Command, Service Cyber Components, Services/Agencies, mission partners, industry, and others. Aside from participation in IPTs (as required), the CDG will require assistance from the Joint Directorates in the following manner:

- J1 - Update manning documents and advocate for joint manpower.
 - Provide manpower assessments and advocate for personnel to support newly developed capabilities.
- J2 - Provide threat assessments to provide context for new requirements.
 - Provide threat assessments for new capabilities to inform concepts of operations (CONOPs) development.
 - Participate in the Integrated Capabilities Requirements Working Group (ICRWG) and assist in describing Intelligence Community-developed capabilities.
- J3 - Identify operational requirements for Cyber Mission Forces.
 - Develop CONOPs for new capabilities.
 - Transition new capabilities to operational forces.
 - Co-chair the ICRWG; prioritize requirements.
- J4 - Provide logistics and facilities support to enable mission execution.

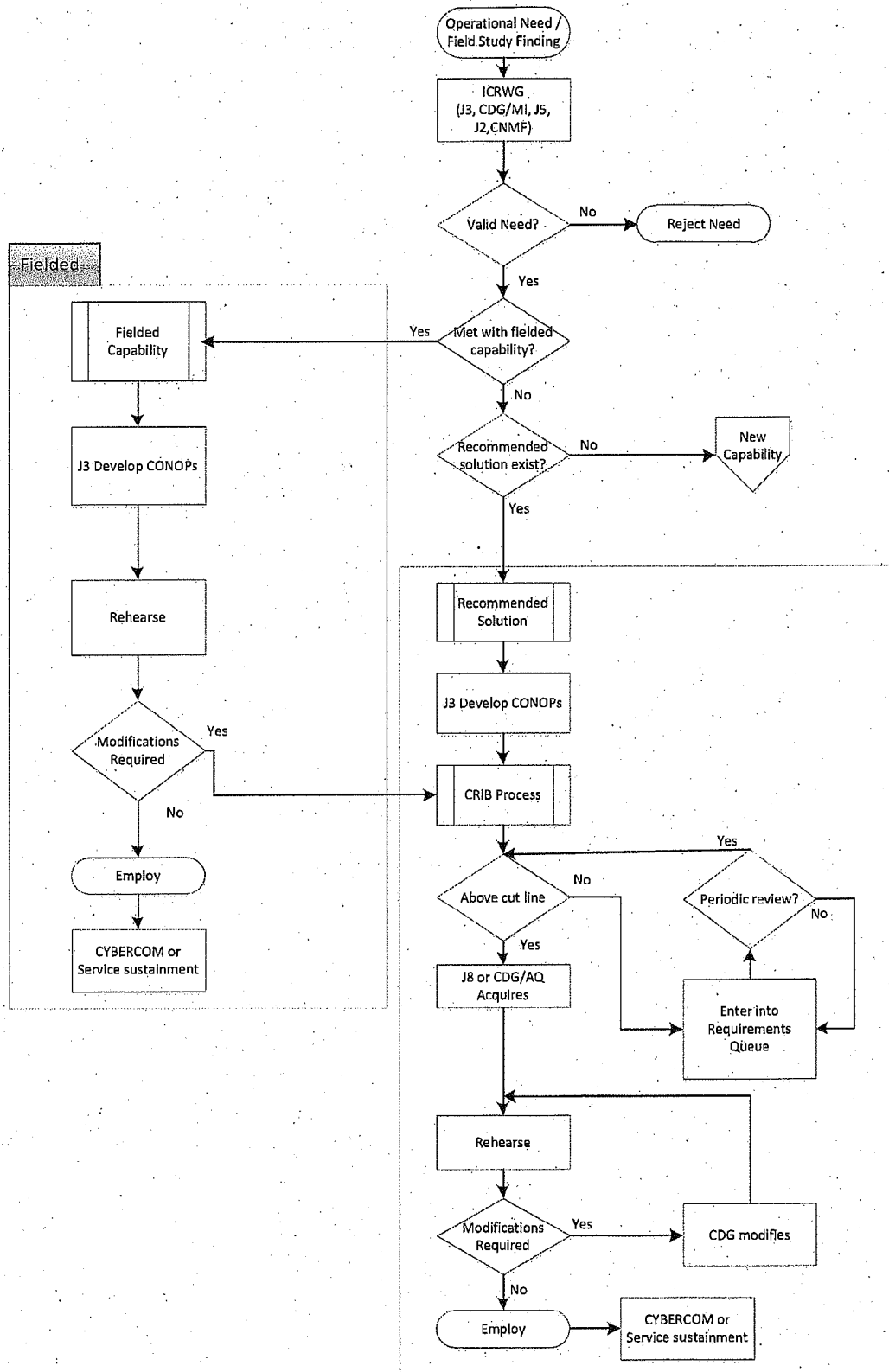
- Participate in the ICRWG as appropriate.
- J5 - Identify requirements from plans.
 - Participate in the ICRWG.
- J7 - Participate in Persistent Training Environment IPT.
 - Coordinate with Cyber Immersion Lab regarding synthetic environments for training and experimentation.
- J8 - Provide budget information to CDG to facilitate spend planning for upcoming fiscal years.
 - Advocate for resources through Program Objectives Memoranda (POM) process.
 - Provide Independent Cost Estimates for proposed solutions.
 - Represent the Command in Functional Capabilities Board(s) and Joint Requirements Oversight Council (JROC).
- Cyber National Mission Force (CNMF)/Joint Force Headquarters - Department of Defense Information Network (JFHQ-DODIN)
 - Identify operational requirements.
 - Participate in ICRWG.
 - Provide participants for experimentation; accommodate field studies.

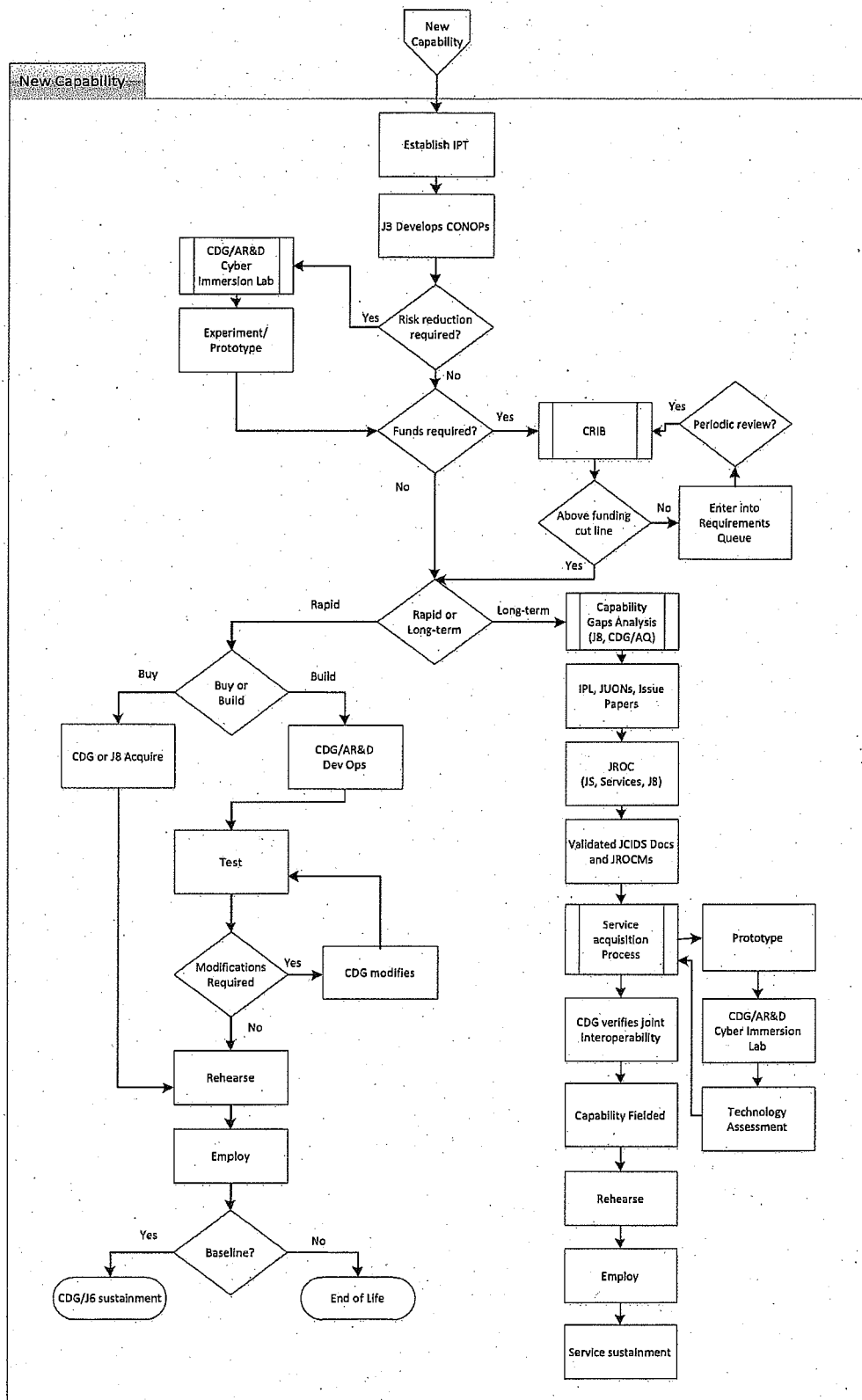
(U//~~FOUO~~) Similarly, CDG personnel will support Command Boards, Bureaus, Centers, Cells, and Working Groups (B2C2WGs) and Directorate specific groups, as necessary. For example, the CDG will provide technical and operational expertise to the development of strategic, campaign, and contingency plans with representation in the J5-led Joint Planning Groups and the J5 Joint Planning Board.

(U//~~FOUO~~) An illustrative process for delivering mission ready capabilities to the Cyber Mission Force is depicted in the flow charts below. The process is subject to Command approval.

- Operational Needs: Operational needs are identified during operations, training, and planning activities. In addition to organizational reporting processes, the CDG sustains a campaign of field study which may further elucidate technology requirements.
- Integrated Capabilities Requirements Working Group: Un-validated requirements based on organizational reporting and field study findings are submitted to the ICRWG. This group, which is co-chaired by J3 and CDG and includes J2, J5, and CNMF representatives, reviews and prioritizes requirements. The ICRWG determines whether the requirement can be met by a fielded capability or a non-fielded existing capability or that a newly developed capability is required.
- Fielded Solution Exists: Fielded capabilities are those which are already deployed for operational use and are sustained by a government organization. For such capabilities, the J3 develops a CONOP, directs mission rehearsals, and employs the capability. If modifications or resources are required, the CDG and J3 submit a Resource Decision Package to the CYBERCOM Requirements and Investments Board (CRIB).

- Non-Fielded Solution Exists: Non-fielded solutions are those which are commercially available or require some investment to deploy, modify or sustain. The J3 develops a CONOP for such recommended solutions and the CDG and J3 submit a prioritized Resource Decision Package to the CRIB. If resources are available, the J8 or CDG acquires and the J3 directs the rehearsal and employment of the capability. The CDG oversees or conducts modifications as required and determines whether the capability will be sustained by USCYBERCOM or should be transitioned to a Service to sustain.
- Newly Developed Capability: For capabilities that must be newly developed, the CDG will establish an integrated product team or incorporate the capability into an existing IPT.
 - A Mission Integrator will lead the IPT, which will consist of subject matter experts from across the Staff and/or subordinate units. The IPT will develop a full requirement description to inform acquisition.
 - The J3 will develop a CONOP and/or use case and the IPT will determine what risk reduction activities (e.g., experimentation or prototyping) are required.
 - CDG/Applied Research & Development will leverage the Cyber Immersion Lab to design and conduct experiments and/or develop prototypes as necessary.
 - If funding is required, the IPT submits a Resource Decision Package along with any results from risk reduction activities to the CRIB.
 - For rapid capability development, the CDG either acquires or develops the capability or the J8 acquires the capability. For capabilities developed internally, CDG/Applied Research & Development conducts test and evaluation prior to providing the capability to the J3 for rehearsals and employment. If the capability is enduring, the CDG/J6 adds it to the technical baseline and sustains it.
 - For deliberate capability development, the CDG assists the J8 with updating the Capability Gap Analysis (CGA).
 - As appropriate, the J8 submits a Joint Urgent Operational Needs Statement (JUON), an Issue Paper, an updated Integrated Priority List (IPL), or Joint Capability Integration and Development System (JCIDS) document to the Joint Staff/Joint Requirements Oversight Council.
 - The JROC validates requirements and capability documents and issues JROC Memorandums (JROCMs), which authorize Service or USCYBERCOM acquisition.
 - For Service developed capabilities, the materiel developer provides the CDG (Cyber Immersion Lab) with prototypes for periodic assessments for operational fit. The CDG verifies joint interoperability. The capability is provided to the Cyber Mission Force. The J3 directs rehearsals and employment. The responsible Service provides life-cycle sustainment.

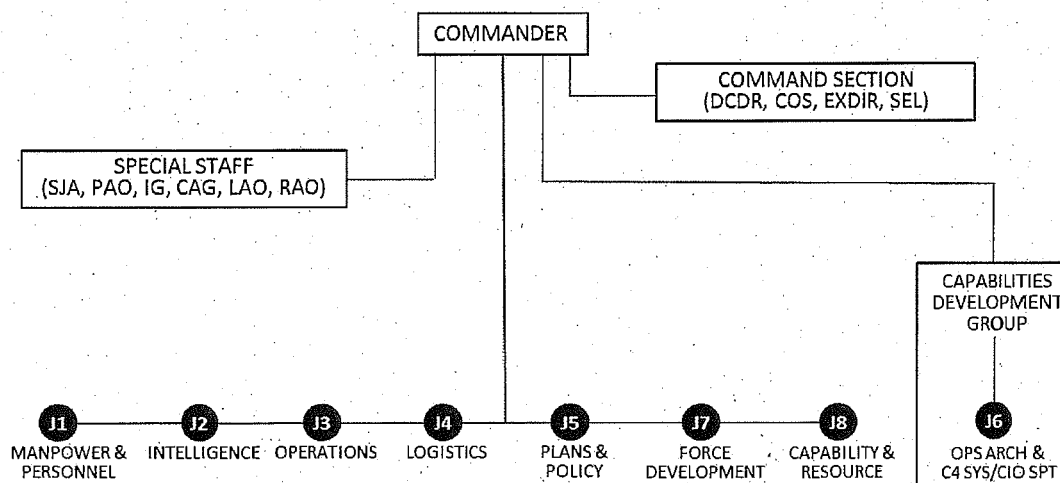




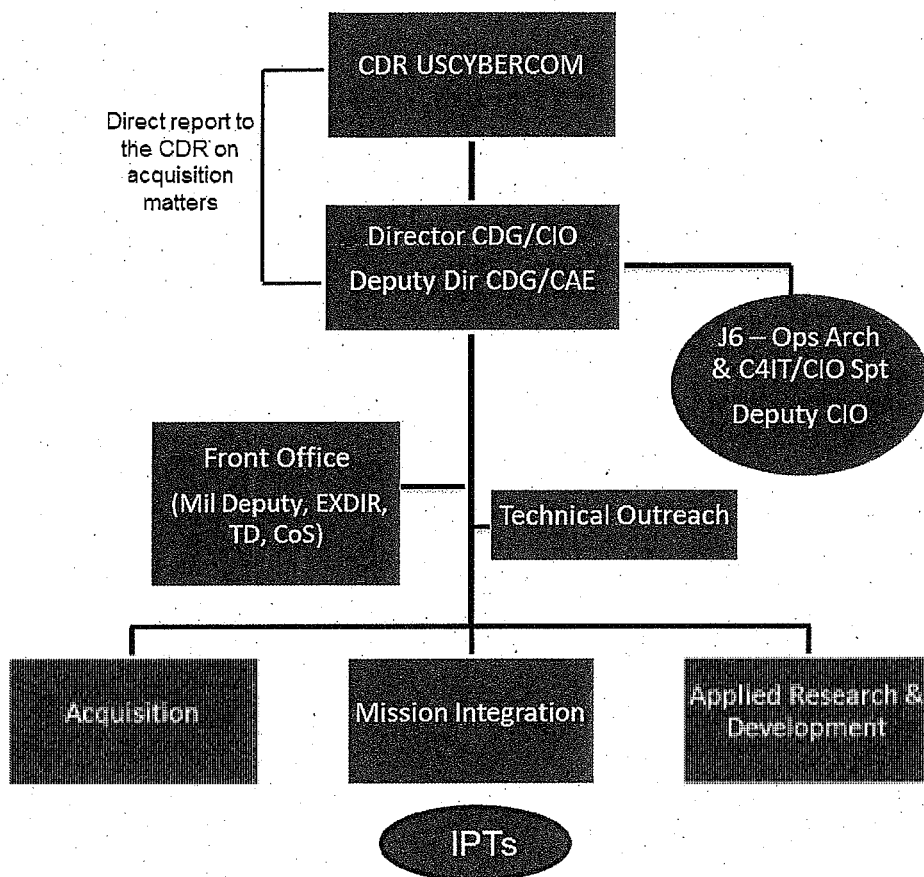
4 (U) Organizational Structure

(U//~~FOUO~~) After examining other organizations that have similar functions envisioned for the CDG, the CDG leadership recommends that the organization most appropriate for the CDG to emulate is United States Special Operations Command's (USSOCOM) Special Operations Forces (SOF) Acquisition, Technology, and Logistics (AT&L). SOF AT&L is a Direct Reporting Unit, reporting directly to the SOCOM Commander, outside of the SOCOM headquarters staff. Note: SOCOM retains the J6 as a Joint Directorate.

(U//~~FOUO~~) As a first step in working towards a similar SOF AT&L construct, the recommended position for the CDG in the USCYBERCOM organizational structure is as a direct report special staff group. As of CDG IOC, the J6 and J9 Directorates were incorporated into the CDG. However, this plan recommends that the J6 Directorate retain its designation, although report to the Commander through the CDG Director. Some of the functions of the J6 will be slightly revised/expanded to support and enable the CDG mission. The benefit of retaining a J6 sub-organization is to facilitate external communications with organizations that traditionally work with a J6. Also, it is possible that in the future, functions that the J6 performs that are primarily in support of capability development could split from the J6 and become a part of the CDG, with the J6 returning to a more traditional J6 role within the Command under the normal staff structure. All of the J9 functions will continue within the CDG; however, the J9 will not retain its designation. The J9 designation in headquarters staffs is not universal and often specified by the Command. Since all of the functions of the J9 in USCYBERCOM are encompassed within the mission of the CDG, this plan recommends not having a separate J9 in order to prevent confusion. The figure below represents the recommended USCYBERCOM headquarters staff structure.



(U//~~FOUO~~) The organizational structure within the CDG is built upon its major functions. The CDG organizational structure is:



(U) Front Office Personnel / Chief Information Officer / Command Acquisition Executive

(U//~~FOUO~~) The Director of the CDG will be a Government Civilian at the Senior Executive Service level or a General/Flag Officer at the two-star level. As directed in the CDG establishment memo, USCYBERCOM's CIO support will reside in the CDG. This plan recommends the CDG Director or Deputy Director, as best qualified, be designated the Command CIO. Furthermore, this plan recommends that initially, the Director be appointed the Command CIO. Also as directed in the CDG establishment memo, the CAE responsibilities will reside within the CDG. This plan recommends the Deputy Director serve as the CAE and will have Milestone Decision Authority (MDA) for developed capabilities if/when it is authorized by Congress and the Secretary of Defense. The CAE will also have a direct reporting function to the Commander, USCYBERCO. Note that as of the date of this implantation plan, no one within the CDG has the required qualifications to fill the CAE role.

(U//~~FOUO~~) The Military Deputy Director will be the senior military member (unless the Director is a military member) to assist the Director in all aspects of CDG functions, with a primary focus on interactions with Department of Defense (DoD) offices.

(U//~~FOUO~~) The Executive Director (Exec Dir) will oversee execution of the CDG mission, help set the vision for the technical baseline of the Command, and broker relationships with key technical communities within the National Security Agency (NSA), Defense Information Systems Agency (DISA), and other partners as applicable.

(U//~~FOUO~~) The Technical Director(s) (TD) will advise the Director on the technical health of the full range of mission areas, including Special Access Programs (SAP) and Special Technical Operations (STO).

(U//~~FOUO~~) The Chief of Staff (CoS) will provide continuous oversight and assessment of the CDG's workload, including identifying issues that require attention by the CDG leadership. The CoS will manage CDG taskings, personnel, and budget tracking actions.

(U//~~FOUO~~) The CDG will designate the senior enlisted member as Senior Enlisted Leader (SEL) of the CDG as an additional duty. In this capacity, this person will serve as the primary advisor to the Director on enlisted personnel matters and provide an enlisted perspective on operational issues. The SEL is responsible for the utilization, training, discipline, readiness, and mission effectiveness of enlisted personnel and will advise the Director on the health, morale, welfare, and quality of life of the directorate workforce.

(U) Technical Outreach

(U//~~FOUO~~) The CDG Technical Outreach team will support the CDG Director on decisions regarding acquiring new cyber capabilities, modifying existing capabilities, or implementing existing solutions to meet warfighting requirements. Their focus will be to establish and manage the team across the Services, research, industry, and academic communities to provide capabilities to the operational force. This focus will be facilitated by their efforts in understanding what those organizations and communities are working on and what they can provide. The Technical Outreach team will provide repository knowledge in this respect to the CDG. An additional effort the Technical Outreach team will undertake is to influence Science and Technology community efforts by articulating USCYBERCOM approved requirements and evaluating the potential of various organizations' abilities to meet them.

(U//~~FOUO~~) Within USCYBERCOM, technical outreach activities will be coordinated with the Command Directorates and the special staff (e.g., Public Affairs, Legislative Liaison, Staff Judge Advocate) including instances of Congressional requests for industry engagements. Technical Outreach will also coordinate with the

Commander's Action Group's (CAG) Point of Partnership personnel to ensure synergistic effects. The Technical Outreach team will rely on the subject matter experts within the CDG to assist in evaluating technologies.

(U//~~FOUO~~) The Technical Outreach team will leverage the engagement activities of other partners to the maximum extent possible and will offer the same courtesy to them, when appropriate, for the benefit of the larger community. Some key relationships are:

- DoD Service capability developers
- DoD Service Research Labs
- Assistant Secretary of Defense for Research and Engineering (ASD(R&E) Cyber)
- Department of Energy (DoE) National Laboratories
- Intelligence Community Capability developers including the National Security Agency and Central Intelligence Agency
- Interagency cyber research and development efforts accessible through membership in Special Cyber Operations Research Engineering (SCORE)
- Academic partners in the cyber research community
- Non-profit technology research companies such as In-Q-Tel
- Intelligence Advanced Research Projects Activity (IARPA) and Defense Advanced Research Projects Agency (DARPA)
- Defense Innovation Unit Experimental (DIUx) and the Point of Partnership field locations
- Industry consortiums such as Armed Forces Communications and Electronics Association (AFCEA) and Washington Cyber Roundtable
- Select industry conferences and workshops cyber related technologies
- Foreign government technology developers

(U) CDG/J6 - Operational Architecture & C4 Systems and CIO Support Directorate

(U//~~FOUO~~) CDG/J6 facilitates the delivery of command, control, communications, computer, and cyber (C4/Cyber) capabilities for USCYBERCOM in support of full-spectrum military cyberspace operations. It provides support to the Command CIO and has expertise in information technology (IT) policy development, project management, architecture development, system engineering, systems administration and accreditation, and data governance.

(U//~~FOUO~~) Specific activities include:

- Build and maintain USCYBERCOM's operational architecture.
- Operate and maintain USCYBERCOM's technical baseline.
- Establish and maintain technical standards consistent with DoD standards to align and integrate USCYBERCOM and Cyber Mission Force capabilities.
- Own and operate the Command Information Assurance program.

- Maintain and enforce the portfolio of CIO governance publications to ensure all USCYBERCOM initiatives are in alignment with higher authority directives.
- Provide data governance, to include a Command Data Steward.
- Provide Enterprise Solution Steering Group (ESSG)/ Cyber Capabilities Working Group (CCWG) support and Information Security Risk Management Committee (ISRMC) Secretariat support.
- Provide Committee of National Security Systems (CNSS) Enterprise Risk Management Board (CERMB) secretariat and external CIO forums and engagements support.
- Manage pooled resources in architecture, systems engineering, technical writing, system administration, and web services to provide matrixed support to USCYBERCOM priority initiatives.
- Surge IT resources in support of exercises, small projects, and major initiatives.
- Provision user accounts, provide reach-through support to service providers, act as subject matter experts for Headquarters systems, and report, prioritize, and respond to critical outages.
- Manage service delivery to mission partners through established capabilities including Battlefield Intelligence Collection Exploitation System (BICES), Mission Partner Environment, and SIPRNet-Releasable (SIPR-Rel).

(U) Applied Research & Development

(U//~~FOUO~~) Applied Research & Development identifies, develops, and assesses capabilities for the Cyber Mission Force and USCYBERCOM. In addition to developing operational capabilities, it develops proofs of concept and prototypes and conducts experiments to reduce risk and orient DoD cyber acquisitions. It operates infrastructure to support experimentation and rapidly develop payloads and analytics. It also provides expertise for cyber developers in the Cyber Mission Force and serves as reachback support to the CNMF.

(U//~~FOUO~~) Specific activities include:

- Operational Tool Development – Develop On Net and Off Net capabilities to support joint operational requirements.
- Data Analytics Development – Develop analytics that can be pushed to network operators and cyber teams to improve decision making.
- Interface and visualization prototyping – Develop proofs of concept for user interfaces and visualizations to orient capability development and support data collection during experiments.
- Experimentation – Conduct empirical assessments of technologies in realistic laboratory or field settings to describe their impacts on decisions and processes.
- Field Studies – Conduct sustained ethnographic research of work in cyber teams and headquarters to document technology requirements, use cases,

and assessment conditions and criteria to inform Experimentation and Mission Integration.

- Test and Evaluation – Conduct performance testing of capabilities that are internally developed.
- Advocate for developer issues to facilitate capability development for the Cyber Mission Force.
- Provide Development and Experiment Environments – Install, provision, and maintain software, hardware, realistic data, and environments to enable development and experiments; use knowledge of networks to inform the design and assessment of technologies.
- Oversee the Joint Capability Development Program (JCDP) – Solicit, review, and approve intern applications; approve JCDP final projects and individual utilization tours; coordinate with National Security Agency's Computer Network Operations Development Program (CNODP) Board of Governors and Program Managers and Executives.

(U//~~FOUO~~) These activities will require a broad array of technical and operational subject matter experts (SME). Using these SMEs, Applied Research & Development will partner with Technical Outreach to triage potential technologies and partners relevant to emerging Command technology requirements.

(U) Mission Integration

(U//~~FOUO~~) Through Mission Integration, the CDG seeks to deliver agile, integrated, coordinated, timely, reliable, supportable, sustainable, and transition-able mission-ready capabilities for the Command and Joint Forces.

(U//~~FOUO~~) Specific activities include:

- Co-chair the ICRWG with J3 to ensure that capabilities are aligned to operational needs and that delivered capabilities and programs are aligned with the Command's plans.
- Partner with operational users to understand their requirements and gaps, identify capability solutions, plan and deliver, or facilitate the delivery of, capabilities, and verify that those capabilities are useable.
- Maintain mission capability portfolios led by a portfolio manager who oversees IPTs within each portfolio.
- Define, create, and maintain IPTs, which will require participation from across the Command, Service Cyber Components, Services/Agencies, mission partners, industry, and others. IPT Leads develop and manage the cost, schedule, and performance mission-ready capabilities being developed by their IPTs.
- Develop capability sustainment and transition plans, working closely with the Services, DISA, etc. to ensure that they are actionable.
- Ensure delivered capabilities integrate with and work seamlessly as part of the Command's operational architecture.

(U//~~FOUO~~) Mission Integration is enabled by Technical Outreach, CDG/J6, Applied Research & Development, and Acquisition to achieve desired outcomes:

- Technical Outreach will identify technologies and partners so that Mission Integration can deliver the most viable capabilities that should be transitioned to the Service's for deployment. Mission Integration will engage with identified partners to manage the specific capability development.
- Applied Research & Development provides findings from field studies that describe technology requirements and use cases. Additionally, it provides prototypes, proofs of concepts, and empirical technology assessments to reduce risk and inform DoD cyber acquisitions.
- CDG/J6 maintains and provides expertise in CIO governance, oversight, information assurance, architecture, system engineering, testing, technical writing, and system administration in support to Mission Capability Portfolios and specific IPTs.
- Acquisition will provide advice on acquisition strategies, assist with acquisition/contracting processes provided by outside Agencies/Services, and provide direct acquisition of cyber-peculiar capabilities (when authorized). Acquisition will also provide cost estimation expertise to support the development of sustainment plans for capabilities developed by IPTs.

(U//~~FOUO~~) Mission Integration is enabled by engagement with DoD components to achieve desired outcomes:

- Mission Integration will partner with the appropriate Service elements to ensure delivered capabilities are designed to be interoperable with existing Service infrastructure, that any Joint capability is built with input from all components, and verify that developed transition plans for capabilities are actionable.
- Mission Integration will engage with OSD components (Acquisition, Technology & Logistics (AT&L), Cost Assessment and Performance Evaluation (CAPE), DoD CIO, etc.), or provide support to another USCYBERCOM Directorates in their engagement, to ensure capability development activities have proper visibility and oversight and are in alignment with department-wide priorities.

(U) Acquisition

(U//~~FOUO~~) Acquisition will support the CAE for capabilities and services developed by the CDG. Acquisition personnel are certified acquisition officials that perform CDG budgetary planning and serve as Contracting Officer Representatives (CORs) for acquisitions. This organization will evolve in conjunction with the Command's acquisition authority as provided in the acquisition authority implementation plan presented to Congress by the Secretary of Defense, in accordance with the FY16 NDAA section 807. The acquisition support functions within the CDG will be matrixed to support multiple IPTs and will house the contractual expertise to enable rapid development and acquisition of capabilities.

(U//~~FOUO~~) Specific activities include:

- Review the cost, schedule, and performance of CDG capability development activities, collating information from across the CDG and partnering organizations.
- Represent the CDG in the CRIB WG to ensure that the CDG has appropriate financial resources to execute its mission on behalf of the Command and Joint Forces.
- Advise the CDG director for the CRIB Executive Committee.
- Support J8 during the IPL and JUON process.
- Provide technical expertise to support J8 during the Issue Paper and Program Budget Review processes.
- Manage acquisition, once authorized.

5 (U) Implementation

(U//~~FOUO~~) For the CDG to be implemented in the manner described in this document, several actions will need to take place. A coordinated Plan of Actions and Milestones (POA&M) for these actions will be delivered to the Commander 30 days after approval of the plan.

6 (U) Plan Approval

(U//~~FOUO~~) This implementation plan is submitted for the Commander's approval.

//Signed//

[Redacted Signature]

Director, Capabilities Development Group
USCYBERCOM

(b) (6)