

CHARTER

National Applications Office

1. PURPOSES

This Charter provides the framework for creating the National Applications Office (NAO), the National Applications Executive Council (NAEC), and the National Applications Domain Committees (DCs). The DCs include the Civil Applications Domain Committee (CADC), the Homeland Security Applications Domain Committee (HSADC), and the Law Enforcement Applications Domain Committee (LEADC).¹ This Charter also creates a Policy and Legal Working Group (PLWG), in addition to the DCs. This Charter also sets forth a process to transition the responsibilities and functions established in the Civil Applications Committee (CAC) Charter to the NAO.

2. APPLICABILITY AND SCOPE

This Charter defines the tasks and responsibilities of each signatory agency that is a party to establishment of the NAO. All activities contemplated under this Charter will be conducted pursuant to the respective authorities and within the mission priorities of the individual Parties to this Charter. This Charter, in and of itself, does not result in transfer of legal authority, appropriated funds, or any other financial obligations among the Parties.

3. BACKGROUND

A. Domestic Use of National Technical Means (NTM). Federal civil agency access to classified remote sensing data for scientific purposes was facilitated from the beginning of national technical programs with the involvement of President Eisenhower's Science Adviser. Through 1972, the use of national overhead systems data for civil, scientific, and environmental purposes was accommodated through the President's Science Advisory Committee (PSAC) under the Science Adviser. In January 1973, President Nixon abolished both the PSAC and the position of Presidential Science Adviser. The lack of federal oversight complicated civil access to classified systems data and products.

B. History of the CAC. Responding to congressional examination of allegations that classified U.S. intelligence collection systems were being used to spy on U.S. citizens, President Ford established the Rockefeller Commission in January 1975. The Commission's task included a review of the entire range of classified overhead photographic sensor capabilities that were being used for imaging domestic areas.

The Rockefeller Commission's review failed to substantiate the allegations of illegal uses of classified imagery and concluded that the existing applications by Federal civil agencies

¹ Although the process of creating the CADC and HSADC may commence once this Charter is signed, this Charter specifies that the LEADC will not be created—and thus the NAO will not accept any requests from the Law Enforcement Domain as defined herein—until such time as all the associated legal, privacy, civil rights, civil liberties, and policy issues have been considered and resolved through the process described below in Section 5.C.

were appropriate and desirable uses of costly nationally funded classified resources. The commission recommended that an interagency committee of Federal civil agencies be established to oversee such applications and to allay concerns about improper or illegal uses of such imaging activities.

An October 3, 1975, memorandum established the “Committee for Civil Applications of Classified Overhead Photography of the United States,” commonly referred to as the CAC. More specifically, the memorandum charged the Secretary of the Interior with establishing the CAC, which, in turn, directed that the U.S. Geological Survey (USGS) chair the CAC.

The CAC includes representatives from the Departments of Interior (DOI), Agriculture (USDA), Commerce (DOC), Transportation (DOT), Health and Human Services (HHS), and Homeland Security (DHS); the U.S. Army Corps of Engineers; the Environmental Protection Agency (EPA); the Federal Emergency Management Agency; the National Science Foundation (NSF); the U.S. Coast Guard; and the National Aeronautics and Space Administration (NASA).

C. CAC Blue Ribbon Study. Recognizing a growing need for the use of Intelligence Community (IC) capabilities in supporting domestic requirements, in May 2005, the Office of the Director of National Intelligence (DNI) (ODNI) and USGS chartered an Independent Study Group (ISG), composed of former senior government and military officials and consultants.

The group conducted an independent review of the future role of the CAC for the facilitation, management, and oversight of remote sensing for civil and/or domestic applications that involve the use of IC capabilities and products. The study also addressed management and processes associated with leveraging IC capabilities against homeland security and law enforcement missions. The ISG concluded that there is “*an urgent need for action because opportunities to better protect the nation are being missed.*”

The ISG found that although the CAC served well the users of civil applications, homeland security and law enforcement users lacked a coherent, organized, and focused process to access IC capabilities. The ISG concluded a new management and process model was needed to employ IC capabilities effectively to support the homeland security and law enforcement communities along with the civil applications community.

The ISG recommended the establishment of the NAO within DHS, with oversight provided by a NAEC. The study results were briefed to all relevant agency and department heads.

The DNI designated the Secretary of DHS Executive Agent and Functional Manager, and formally endorsed the establishment of the NAO to serve as an independent advocate for, and facilitate access to, IC capabilities by non-traditional users of intelligence. In a letter dated June 29, 2007, the DNI asked each IC element to work with the DHS and the NAO to ensure successful implementation of the NAO.

4. ESTABLISHMENT AND MISSION

This Charter establishes the NAO as an advocate for IC capabilities to serve, among others, non-traditional users in the civil, homeland security, and law enforcement communities. The NAO will advocate for future technology needs of these communities to the IC. It will collaborate with these potential users about IC capabilities and how and when they might best be leveraged to support their needs in accordance with existing legal, privacy, civil rights, civil liberties, and policy requirements.

5. RESPONSIBILITIES

A. National Applications Office. The NAO has eight primary functions:

(1) Facilitate Access to IC Capabilities

- Receive, evaluate, consolidate, and prioritize requests for IC capabilities from DCs and participants (as defined in Appendix A)
- Conduct legal reviews of all requests for access to IC capabilities or archived data to determine whether such access is consistent with the U.S. Constitution and existing laws, policies, and procedures
- Submit validated and approved requests to appropriate IC entities for collection or response
- Facilitate DC and participants' requests for the processing, analysis, and dissemination of data and information
- Facilitate access to archived data

(2) Facilitate Lawful and Appropriate Use of IC Capabilities

- Provide guidance regarding access to IC capabilities and archived data that is consistent with the Constitution, and other legal authorities
- Assist DCs and participants in adhering to appropriate laws, policies, and directives to govern their use of IC capabilities
- Coordinate with the appropriate offices within DHS, the Department of Justice (DOJ), ODNI, the Department of Defense (DoD) and the applicable IC Functional Manager on any requests for the use of IC capabilities or access to archived data that involve significant or novel legal questions to ensure appropriate legal and policy reviews of such requests. The Attorney General shall serve as the final arbiter of such legal questions.

(3) Safeguard Privacy, Civil Rights, and Civil Liberties

- Ensure the NAO's and its Committees' procedures are in accordance with laws, policies, and procedures that protect privacy, civil rights and civil liberties, including:
 - The U.S. Constitution
 - Executive Order 12333 and the procedures for IC members under that order that have been approved by the Attorney General
 - The Posse Comitatus Act
 - The Privacy Act of 1974, as amended

- The E-Government Act of 2002, Section 208
- The Homeland Security Act of 2002, Section 222, as amended
- Any other applicable laws, policies, or procedures that have the purpose or effect of safeguarding privacy, civil rights, or civil liberties
- Provide regular guidance and training — on applicable laws, policies, and procedures that protect privacy, civil rights, and civil liberties — to NAO personnel and appropriate IC or other personnel involved in providing assistance to the NAO. Such guidance and training shall specifically address policies and procedures for:
 - The use of any IC capability that would, if used for law enforcement purposes inside the United States, require a warrant or court order;
 - Determining whether and under what circumstances IC capabilities may be directed at specific United States persons; and
 - Determining whether and under what circumstances, consistent with the Posse Comitatus Act, assets of a DoD agency may be used for domestic law enforcement, homeland security, or regulatory purposes.

(4) Promote Effective and Efficient Use of IC Assets

- Facilitate the sharing and use of data
- Consider new or unique uses of IC capabilities and facilitate access to them
- Promote the use of unique analytical methodologies or technology in solving civil, homeland security, or law enforcement problems
- Encourage long-term data management and archiving by Functional Managers pursuant to their respective authorities
- Coordinate IC outreach to provide technical, educational, and analytical support to the DCs

(5) Promote Information Sharing

- Inform DC participants about the proper use and limitations on information derived from commercial and IC assets
- Assist the DCs in understanding the process to request and use IC capabilities
- Educate the IC on the information needs and the capabilities of the Domains
- Educate the Domains on the capabilities of the IC
- Facilitate mutual awareness of research and development activities between the IC and the Domains
- Facilitate training on sources and methods protection to NAO customers

(6) Protect Sources and Methods

- Incorporate mechanisms into all DCs and NAO activities that protect intelligence sources and methods according to law, regulations, orders, directives, and the guidelines established by the DNI and the IC Functional Managers for uses of their respective systems
- Incorporate mechanisms into all DCs and NAO activities that promote the legal and appropriate handling and coordination of classified, restricted, and licensed information and proprietary business interests

(7) Provide Representation

- Advocate to the IC of the domain participants' NAO mission-related budget requests for discussing new collection and analytic capabilities
- Act as the tasking, collection, processing, analysis, and dissemination advocate between the Domain participants and the IC
- Serve as advocate for the Domain participants in IC fora approving the acquisition of new intelligence systems and exploitation capabilities
- Provide the DCs with administrative support, such as document control, scheduling meetings, and handling logistics
- Report after the first six months of operation and then annually to the NAEC on activities, plans, and recommendations

(8) Sponsor Applications of National Capabilities Program

- The NAO will sponsor an Applications of National Capabilities Program (ANCAP), modeled after the DoD Tactical Exploitation of National Capabilities Program (TENCAP), for the NAO community to help integrate applications in the domains and ensure future evolution and development of systems and techniques.

B. National Applications Executive Council. The NAEC will oversee the NAO. Tri-chaired by the Deputy Secretary of DHS, the Deputy Secretary of DOI, and the Principal Deputy DNI, it will be composed of senior-level agency representatives from the principal DCs and the IC, aided by their policy, legal, privacy, and civil liberties and civil rights advisors. Members of this Council will monitor the NAO's performance, assist in fostering innovation, and seek to resolve issues arising in program and mission execution, whether manifested in operations, policy, or law.

The NAEC shall have full authority to adjust any aspect of the NAO's operation, including NAEC membership. In the event that there are any significant issues that cannot be resolved by the NAEC, such issues will be referred to the Secretaries of Homeland Security, Defense, and Interior, the DNI, and the Attorney General for discussion and resolution. The National Security Council (NSC), Homeland Security Council (HSC), and Domestic Policy Council (DPC) Deputies Committees and their staffs may assist in coordination, as necessary.

The NAEC membership will consist of the following: DoD, DOJ, DOC, Department of Energy (DOE), USDA, DOI, HHS, DOT, and DHS, the ODNI, EPA, NASA, and NSF.

C. Domain Committees. The DCs will advise the Director of the NAO regarding strategic priorities, process improvements, and customer satisfaction. Some members may have missions in more than a single domain and may, therefore, participate in more than one DC. DCs will meet to discuss and to promote common interests. The DCs have the flexibility to adjust their structure and membership to ensure maximum access to IC capabilities by Domain users.

The Law Enforcement Applications DC will not be created—and thus the NAO will not accept any requests from the Law Enforcement Domain—until the PLWG has considered

and resolved all the associated legal, privacy, civil rights, civil liberties, and policy issues to the satisfaction of the NSC, HSC, and DPC (at the level of the Deputies Committees or higher). As stated in Appendix A, the Law Enforcement Domain includes law enforcement entities when they are seeking to enforce criminal or civil laws or investigate violations thereof. When law enforcement entities are not so focused, their activities may fall within the Homeland Security Domain.

In partnership with the NAO, the DCs will:

- (1) Advise the Director, NAO, regarding Domain priorities
- (2) Receive and evaluate requests for IC capabilities from committee member organizations
- (3) Suggest process improvements and gauge customer satisfaction to identify best practices
- (4) Serve as fora to exchange information and educate the customer base on the capabilities of, and relevant policy and legal constraints on, use of IC capabilities
- (5) Vote on long-term domain projects and prioritization of long-term requirements
- (6) Educate the IC to increase understanding of the requirements and capabilities of the Domain participants
- (7) Inform the NAO of their Domain mission-related rules and regulations
- (8) Play a key role in the prioritization, approval, and monitoring of projects selected under the ANCAP
- (9) Submit requests to the NAO for access to IC capabilities

D. Policy and Legal Working Group. The PLWG, co-chaired by ODNI and DHS with representatives from the IC, DOJ, DoD, and other relevant legal, policy, civil liberties, and privacy offices, shall be created to provide a readily available forum to discuss and resolve policy and legal issues identified or raised during NAO mission execution.

6. IC CAPABILITIES

Intelligence capabilities comprise those resources used to task, collect through technical means, process, analyze, or disseminate information in response to requirements, to the extent authorized by Executive Order 12333 and other applicable authorities. The NAO will facilitate access to geospatial intelligence (GEOINT), measurement and signature intelligence (MASINT), open-source intelligence information, and non-communications technical signals known as electronic intelligence (ELINT). See Appendix A for the definitions of the IC disciplines and capabilities.

7. EXCLUSIONS

The NAO will have no authority to accept requests to use IC capabilities to intercept or acquire communications, including those covered by Title III of the Omnibus Safe Streets and Crime Control Act of 1968 or the Foreign Intelligence Surveillance Act (FISA). The NAO will refer any questions about the applicability of FISA or the interception or acquisition of communications to DOJ.

8. HOW THE NAO FUNCTIONS

A. General. As an independent advocate, the NAO encourages integrated, multi-agency solutions to leverage the IC's capabilities for support of non-traditional users of intelligence. Since it provides a consistent process for all parties, the customer does not need to have a detailed knowledge of the IC or its capabilities to obtain necessary and relevant information.

The NAO is designed to assist a wide variety of customers. The DHS Offices of Privacy, Civil Rights and Civil Liberties, Policy, and General Counsel, along with the ODNI's Civil Liberties and Privacy Office, will provide support and guidance to the NAO and recommend measures to ensure that the use of domestic information respects and protects the privacy and civil liberties of U.S. persons. Furthermore, officers in each IC Functional Manager will carry out final legal and policy reviews of all NAO-approved requests for IC-provided information within their respective functional areas.

B. Requirements Processing. As an initial matter, to expedite the below review process, any Domain member requesting the use of the IC's technical intelligence capabilities through the NAO will submit to the pertinent IC Functional Manager an annual memorandum that defines in advance its requirements and intended uses, including the legal and policy restrictions governing use of any information provided. Once such a memorandum is in place, the process will begin with the customer submitting a request to the NAO and in parallel to the appropriate DC. This may be accomplished where such a memorandum is not in place through a one-time request. The NAO or DC will determine first whether there are intelligence capabilities available to apply to the problem. The NAO then will evaluate the request to ascertain that the use falls within the legal authorities of both the requesting and providing agencies and that it is consistent with applicable laws, regulations, directives, orders, and policies. This will be accomplished by the appropriate legal office of the requesting entity verifying that the request is lawful and made for a proper purpose (i.e., it is necessary for the execution of an authorized entity mission).

The request will then be reviewed by the NAO staff attorney in coordination with the office of general counsel at the collecting agency. Where collection requires a warrant or order, the NAO will only recommend approval of that requested use on the condition that the requesting entity obtains a warrant or order.

Moreover, the NAO staff will screen the proposed uses to identify any special uses that require additional scrutiny. Where a proposed use falls within any of the special use categories listed below, the NAO staff will then coordinate with DOJ and other departments and agencies, including DHS and ODNI and the IC Functional Manager, for further legal, privacy, civil rights, and civil liberties review. DOJ shall be the ultimate arbiter of any associated legal questions. The special use categories are as follows:

- The collection is requested for or reasonably expected to reveal information about the activities of U.S. persons.

- The collection supports any statutory and authorized law enforcement function performed by any organization, agency, or department.²
- The collection supports a regulatory enforcement organization or purpose, or could reasonably be expected to support or become involved in regulatory enforcement proceedings.
- The anticipated use of collected information is likely to result in a request to disclose classified sources or methods or presents a risk of unapproved disclosure of such sources and methods.
- The nature of the information collected is intrusive or raises privacy or civil rights and civil liberties issues.
- The requested collection otherwise raises novel or significant legal or policy issues or seeks access to archived data.

The NAO will then employ the proper specific procedures, as required.

After this screening, the NAO will determine whether to endorse the request and how it should be prioritized. If it is assessed that the request may fit in one of the above categories, this will be highlighted in the request package that is forwarded to the appropriate IC Functional Manager for review and final decision.

If the NAO agrees to sponsor the request, the NAO will request support from the agency with the relevant capability. If that agency agrees to provide support, NAO will then monitor the tasking, collection, processing, analysis, and dissemination cycle of the request to facilitate customer receipt of the requested product. Throughout, there will be feedback between the customer, the producer, and the NAO, to communicate the status of the project and deliverables.

Furthermore, any potential applications of new technologies or current technologies not in common use by law enforcement, homeland security, or other organizations that implicate the Fourth Amendment to the U.S. Constitution will be reviewed in the manner described above for significant and novel legal questions.

² Executive Order 12333, section 2.6, authorizes the IC to provide limited support to law enforcement authorities. With regard to the NAO, the Intelligence Community may: (1) provide specialized equipment, technical knowledge, or assistance of expert personnel for use by any department or agency, except local law enforcement agencies; (2) when lives are endangered, provide specialized equipment, technical knowledge, or assistance of expert personnel to support local law enforcement agencies; and (3) render any other assistance and cooperation to law enforcement authorities not precluded by applicable law. The provision of assistance by expert personnel must be approved in each case by the General Counsel of the providing agency.

This process does not relieve the relevant customer, DCs, supporting agencies, and the IC Functional Manager of their independent obligations to observe their own agency regulations and applicable legal and policy requirements governing the collection, use, and dissemination of information.

9. RESPONSIBILITIES OF THE PARTIES TO THIS CHARTER

By signature of this Charter, the signatory parties have agreed to the responsibilities set forth herein.

A. DHS will:

- (1) Serve as the Executive Agent and Functional Manager for the NAO. In executing this responsibility, DHS, in partnership with the ODNI and all relevant stakeholders, will develop and coordinate an organizational construct for the NAO, ensure resource requirements are identified and opportunities are provided for multiple organizations to participate, and develop operational procedures
- (2) Provide a senior-level tri-chair for the NAEC
- (3) Provide the chair of the HSADC
- (4) Provide a homeland security subject-matter expert to the NAO Staff
- (5) In coordination with DOI, develop the process for, and facilitate the transition of, the functions and responsibilities of the CAC to the NAO
- (6) Provide funding for NAO facilities, operations, and support to the NAEC and DCs, except as otherwise provided in this Charter or by separate agreement
- (7) Designate a legal counsel to support the NAO with the necessary expertise

The Secretary of DHS will be responsible for the operations of the NAO and the proper exercise of the functions listed above.

B. DOI will:

- (1) Continue to provide administrative and facilities support, as appropriate, for the CAC, the CAC Secretariat, and the CAC Executive Steering Group until their transition is complete
- (2) Provide a senior-level tri-chair for the NAEC
- (3) Provide the chair of the CADC
- (4) Provide a civil applications subject-matter expert to the NAO Staff
- (5) In coordination with DHS, develop the process for and facilitate the transition of, the functions and responsibilities of the CAC to the NAO. DOI will continue to operate the CAC until DHS has demonstrated that services rendered under the CAC can continue uninterrupted under the NAO
- (6) Provide a Deputy Director for the NAO
- (7) Provide on a reimbursable basis the initial facility that may be used by the NAO at the USGS Advanced Systems Center, in Reston, Virginia

C. DOJ will:

- (1) Provide the chair of the LEADC
- (2) Provide a law enforcement subject-matter expert to the NAO Staff
- (3) Review any request that raises significant or novel legal questions, including requests within any of the special use categories listed above in Section 8.B., and serve as the final arbiter of such legal questions and of the legality of such requests

D. ODNI will:

- (1) Provide a senior-level tri-chair for the NAEC
- (2) Coordinate, review, and approve the development of IC policies and procedures to assist Domain members and IC Functional Managers in support of the NAO mission
- (3) Provide National Intelligence Program (NIP) funding as appropriate
- (4) Facilitate NAO and Domain members understanding of existing laws, Executive Orders, and policies that affect NAO functions

E. DoD will:

- (1) Provide a senior-level representative to the NAEC
- (2) Provide representatives to the DCs
- (3) Provide representatives to the Policy and Legal Working Group
- (4) Designate the senior DoD representative for all NAO groups and forums
- (5) Coordinate with the NAO, DOJ, ODNI, and applicable IC Functional Managers to facilitate appropriate requests, as appropriate, to:
 - o Collect, process, analyze, or disseminate data using assets operated by DoD personnel
 - o Analyze data using DoD personnel
 - o Access archived data held by DoD
- (6) In appropriate circumstances, consider waiver of the reimbursement requirement for requests that:
 - o May be handled through the normal course of military training or operations, or
 - o Result in a benefit to DoD that is substantially equivalent to that which would otherwise be obtained from military operations or training
- (7) Assist the NAO with expertise, as requested, with the Applications of National Capabilities Program

10. IMPLEMENTATION

A. Implementation of Responsibilities. Each of the agencies and offices referenced above shall implement their responsibilities under this Charter in accordance with all applicable laws, regulations, orders, directives, and policies. Any responsibility or duty assigned herein to the signatories may be delegated to one or more subordinate officials at the discretion of the official to whom the authority or duty is assigned, except as otherwise provided in this Charter or limited elsewhere.

B. Timelines. NAO's operating capability will commence once the Charter signatories officials agree that appropriate procedures are in place to conduct NAO operations in accordance with applicable laws, regulations, policies, and procedures. The DC structures will be established and begin operations when practicable and certified legally sufficient by the NAO legal advisor and approved by the NAEC. As stated above in Section 5.C., the LEADC will be established at a later date, once all legal and policy issues have been considered and resolved.

DOI will continue to operate the CAC until DHS, ODNI, and DOI reach agreement that functional capabilities, outlined in the transition plan, have been demonstrated to the degree that services rendered under the CAC can continue uninterrupted under the NAO. The CAC Charter will expire and all functions and responsibilities will be transferred to the NAO or the NAEC, as appropriate, upon successful implementation of a capabilities-based transition plan. Prior to this transition, the NAEC will establish to the satisfaction of the NSC, HSC, and DPC (at the level of the Deputies Committees or higher) that DHS is capable of undertaking its duties under this Charter.

C. Disestablishment of the CAC. Upon the expiration of the CAC Charter, as provided for in Section 10.B. above, the CAC Charter will be a historical reference for the civil functions of the NAO.

11. FUNDING

Cooperative activities under this Charter shall be subject to the availability of appropriated funds and resources and undertaken in accordance with existing legal authorities. This Charter shall not be construed to obligate any particular expenditure or commitment of funds and/or resources. Funds or resources may be provided by the parties to support activities under this Charter when authorized by law, and consistent with applicable regulations. The provision of such funds and resources will be accomplished through separate written agreements, as needed.

12. EFFECTIVE DATE, MODIFICATION, AND TERMINATION

This Charter is effective the day the last signatory signs it, and it remains in effect until cancelled or superseded by mutual consent of the signatories in writing. To withdraw as a party to the Charter, that party must provide all other parties written notice 30 days in advance. This Charter may be modified in writing at any time by mutual consent of the parties.

13. COUNTERPART SIGNATURES

This Charter may be signed in counterparts, each of which shall be considered to be an original.

Attorney General

Date

Director of National Intelligence

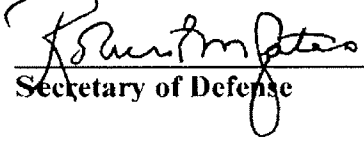
Date

Secretary of Homeland Security

Date

Secretary of the Interior

Date



Secretary of Defense

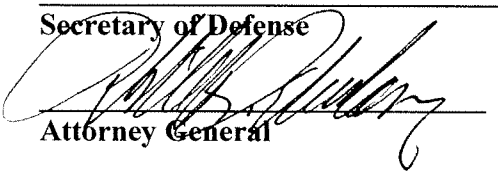
FEB 22 2008
Date

C. Disestablishment of the CAC. Upon the expiration of the CAC Charter, as provided for in section 10.B above, the CAC Charter will be a historical reference for the civil functions of the NAO.

11. FUNDING. Cooperative activities under this Charter shall be subject to the availability of appropriated funds and resources. Beyond the obligations specifically noted, this Charter shall not be construed to obligate any particular expenditure or commitment of funds and/or resources. Funds or resources may be provided by the parties to support activities under this Charter when authorized, and consistent with applicable regulations. The provision of such funds and resources will be accomplished through separate written agreements, as needed.

12. EFFECTIVE DATE, MODIFICATION, and TERMINATION. This Charter is effective the day the last signatory signs and it remains in effect until cancelled or superseded by mutual consent of the signatories in writing. To withdraw as a party to the Charter, that party must provide all other parties written notice 30 days in advance. This Charter may be modified in writing at any time by mutual consent of the parties.

13. COUNTERPART SIGNATURES: This Charter may be signed in counterparts, each of which shall be considered to be an original.

Secretary of Defense


Attorney General

Date
2/4/08

Date

Secretary of the Interior

Date

Secretary of Homeland Security

Date

Director of National Intelligence

Date

C. Disestablishment of the CAC. Upon the expiration of the CAC Charter, as provided for in section 10.B above, the CAC Charter will be a historical reference for the civil functions of the NAO.

11. FUNDING. Cooperative activities under this Charter shall be subject to the availability of appropriated funds and resources. Beyond the obligations specifically noted, this Charter shall not be construed to obligate any particular expenditure or commitment of funds and/or resources. Funds or resources may be provided by the parties to support activities under this Charter when authorized, and consistent with applicable regulations. The provision of such funds and resources will be accomplished through separate written agreements, as needed.

12. EFFECTIVE DATE, MODIFICATION, and TERMINATION. This Charter is effective the day the last signatory signs and it remains in effect until cancelled or superseded by mutual consent of the signatories in writing. To withdraw as a party to the Charter, that party must provide all other parties written notice 30 days in advance. This Charter may be modified in writing at any time by mutual consent of the parties.

13. COUNTERPART SIGNATURES: This Charter may be signed in counterparts, each of which shall be considered to be an original.

Secretary of Defense

Date

Attorney General

Date

Secretary of the Interior

Date

Secretary of Homeland Security

February 6, 2008

Date

Director of National Intelligence

Date

C. Disestablishment of the CAC. Upon the expiration of the CAC Charter, as provided for in section 10B above, the CAC Charter will be a historical reference for the civil functions of the NAO.

11. FUNDING

Cooperative activities under this Charter shall be subject to the availability of appropriated funds and resources. Beyond the obligations specifically noted, this Charter shall not be construed to obligate any particular expenditure or commitment of funds and/or resources. Funds or resources may be provided by the parties to support activities under this Charter when authorized, and consistent with applicable regulations. The provision of such funds and resources will be accomplished through separate written agreements, as needed.

12. EFFECTIVE DATE, MODIFICATION, and TERMINATION

This Charter is effective the day the last signatory signs and it remains in effect until cancelled or superseded by mutual consent of the signatories in writing. To withdraw as a party to the Charter, that party must provide all other parties written notice 30 days in advance. This Charter may be modified in writing at any time by mutual consent of the parties.

13. COUNTERPART SIGNATURES

This Charter may be signed in counterparts, each of which shall be considered to be an original.

Attorney General

Date

Director of National Intelligence

Date

Secretary of Homeland Security

Date



Secretary of the Interior

2-5-08

Date

Secretary of Defense

Date

C. Disestablishment of the CAC. Upon the expiration of the CAC Charter, as provided for in section 10.B above, the CAC Charter will be a historical reference for the civil functions of the NAO.

11. FUNDING. Cooperative activities under this Charter shall be subject to the availability of appropriated funds and resources. Beyond the obligations specifically noted, this Charter shall not be construed to obligate any particular expenditure or commitment of funds and/or resources. Funds or resources may be provided by the parties to support activities under this Charter when authorized, and consistent with applicable regulations. The provision of such funds and resources will be accomplished through separate written agreements, as needed.

12. EFFECTIVE DATE, MODIFICATION, and TERMINATION. This Charter is effective the day the last signatory signs and it remains in effect until cancelled or superseded by mutual consent of the signatories in writing. To withdraw as a party to the Charter, that party must provide all other parties written notice 30 days in advance. This Charter may be modified in writing at any time by mutual consent of the parties.

13. COUNTERPART SIGNATURES: This Charter may be signed in counterparts, each of which shall be considered to be an original.

Secretary of Defense


Date

Attorney General

Date

Secretary of the Interior

Date

Secretary of Homeland Security


Director of National Intelligence

Date
12 FEB 08

Date

APPENDIX A

DEFINITIONS

Applications of National Capabilities Program. The NAO will sponsor an Applications of National Capabilities Program (ANCAP), modeled after the DoD Tactical Exploitation of National Capabilities (TENCAP) Program, for the NAO community to help integrate applications in the domains and ensure future evolution and development of systems and techniques. ANCAP will foster new and innovative technology-related ideas for the use of IC capabilities in meeting Civil, Homeland Security, and Law Enforcement needs.

Civil Applications Domain. The “Civil Applications Domain” (CA) includes Federal civil agencies and other entities involved with domestic and international research, analysis, and operations designed to support the assessment of climate variability and change, management of federal lands and water, the wise use of natural resources, the monitoring of environmental conditions, analyzing global dynamic processes, evaluating socioeconomic conditions, producing maps and charts, conducting risk assessments, mitigating threats, preparation for, responding to, and supporting recovery/rehabilitation actions with regard to disasters.

Domain. The word “Domain” refers to a customer community that could use intelligence capabilities in support of its missions. Three such domains are described in this document: Civil Applications, Homeland Security, and Law Enforcement.

Domestic Imagery. Any imagery collected from classified national reconnaissance platforms covering the 50 United States, the District of Columbia, and territories and possessions of the United States to a 12-nautical mile seaward limit of the land areas.

Electronic Intelligence (ELINT). The word “ELINT” refers to technical and geolocation intelligence derived from foreign non-communications electromagnetic radiations emanating from other than nuclear detonations or radioactive sources.

Geospatial Intelligence (GEOINT). GEOINT is statutorily defined in 10 U.S.C. 467 as the exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the Earth. Geospatial intelligence consists of imagery, imagery intelligence, and geospatial information.

Homeland Security Domain. The “Homeland Security Domain” (HS) includes those government agencies and activities involved in the prevention and mitigation of, preparation for, response to, and recovery from natural or man-made disasters, including terrorism, and other threats to the homeland. This domain can encompass the many operational and administrative components of DHS, as well as other Federal, state, local, territorial, and tribal entities who partner with DHS. The NAO shall not abrogate any of the functions of the Joint Terrorism Taskforces (JTTF), Field Intelligence Groups, or the National JTTF.

Law Enforcement Domain. The “Law Enforcement Domain” (LE) includes Federal, state, local, territorial, and tribal law enforcement entities to the extent those entities are enforcing criminal or civil laws or investigating violations thereof. Prior to the establishment of the LEADC, the NAO will not accept any requests from state, local, tribal, and territorial law enforcement entities, even if the subject of such requests properly resides in the Homeland Security Domain.

Measurement and Signature Intelligence (MASINT). Scientific and technical intelligence produced by quantitative and qualitative analysis of physical attributes of targets and events in order to characterize and identify them.

Open source intelligence information. Open source information is produced from publicly available information that is collected, analyzed, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement. Open source information is publicly available information that anyone can lawfully obtain by request, purchase, or observation.

Remote Sensing. Acquiring information about an object or target using a recording device that is not in physical proximity with the object under study.

APPENDIX B

REFERENCES AND AUTHORITIES

REFERENCES

- A. Title III of the Omnibus Safe Streets and Crime Control Act of 1968, as amended, 18 U.S.C 2510 et seq.
- B. Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. 1801 et seq.
- C. Posse Comitatus Act, 18 U.S.C. 1385
- D. Charter, Committee on Civil Applications of Classified Overhead Remotely Sensed Data, October 2, 2000
- E. CAC Blue Ribbon Study Independent Study Group Final Report, September 2005
- F. Director of National Intelligence (DNI) Memorandum, Designation of Executive Agency for the National Applications Office, May 25, 2007 (SECRET)
- G. Secretary, Department of Homeland Security (DHS), Delegation 8500, "Delegation of Authority for the Establishment and Management of the National Applications Office," signed August 17, 2007
- H. Executive Order 12333, United States Intelligence Activities, December 4, 1981
- I. Letter dated February 22, 2007, from Paul Schneider, DHS Under Secretary for Management, to David Price, Chairman, Subcommittee on Homeland Security Committee on Appropriations, regarding Section 503(a)(1) of FY 2007, Department of Homeland Security Appropriations Act Notification (SECRET//NOFORN)
- J. Letter dated April 20, 2007, from David Price, Chairman, Subcommittee on Homeland Security Committee on Appropriations, to Paul Schneider, DHS Under Secretary for Management, responding to Department's February 22, 2007, request (SECRET//NOFORN)
- K. Letter dated July 17, 2007, from David Price, Chairman, Subcommittee on Homeland Security Committee on Appropriations, to Michael Chertoff, DHS Secretary, responding to Department's February 22, 2007, request (SECRET//NOFORN)

AUTHORITIES

In addition to the organic authorities of requesting and collecting entities, the NAO will rely on the following authorities:

- A. Executive Order 12333, "United States Intelligence Activities" December 4, 1981
- B. Economy Act, 31 USC 1535
- C. National Security Act of 1947, as amended, 50 USC 401 et seq.
- D. Homeland Security Act of 2002, 6 USC 111 et seq.
- E. Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458
- F. Secretary, Department of Homeland Security (DHS), Delegation 8500, "Delegation of Authority for the Establishment and Management of the National Applications Office," signed August 17, 2007