UNCLASSIFIED

Civil Applications Committee (CAC) Blue Ribbon Study

Independent Study Group Final Report

September 2005

This document was produced for the sole use of the U.S. government

UNCLASSIFIED

Independent Study Group Members

Mr. Keith Hall
Chairman
Vice President, Booz Allen Hamilton

Edward G. Anderson
LTG US Army (Ret)
Principal
Booz Allen Hamilton

Jeff Baxter
Independent Consultant

Thomas W. Conroy
Vice President,
National Security Programs
Northrop Grumman/TASC

Dr. Paul Gilman
Director,
Oak Ridge Center for
Advanced Studies

Patrick M. Hughes
LTG US Army (Ret)
Vice President, Homeland Security
L-3 Communications

Kemp Lear
Associate
Booz Allen Hamilton

Kevin O'Connell
Director,
Center for Intelligence
Research and Analysis

Joseph D. Whitley, Esq.
Alston & Bird, LLP

Executive Secretariat:

Booz Allen Hamilton:
- Mr. Greg Jay
- Mr. Bob Evans
- Mr. Chuck Symes
- Mr. Ed Obloy
- Ms. Robin Saenz

Government:
- Mr. Keith Elliot, USGS
- Mr. Marty Eckes, USGS
- Mr. Randy Soderholm, ODNI

INDEX

Executive Summary p. 4

Chapter 1: Introduction p. 6

Chapter 2: Findings and Recommendations p. 10

a. **Finding Number 1** p. 10
LE & HLS lack a coherent process to access IC capabilities.

b. **The Model** p. 13
i. Governance p. 14
ii. Policy and Legal p. 18
iii. Requirements Flow p. 19
iv. Metrics p. 22
v. Budget Authority p. 22
vi. Training and Education p. 23

c. **Finding Number 2** p. 24
CAC process should serve as a model for a future process.

d. **Finding Number 3** p. 26
Many domestic users are unsure how to use IC capabilities.

e. **Finding Number 4** p. 26
Domestic user's requirements must be addressed in any future acquisition process.

f. **Finding Number 5** p. 29
IC domestic use policies reflect pre-9/11 environment.

g. **Finding Number 6** p. 32
Domestic use of geospatial data is impeded by policy/classification barriers.

h. **Finding Number 7** p. 35
Overlapping jurisdictions complicates support to domestic users.

i. **Finding Number 8** p. 37
Domestic information use is complicated by special handling rules.

j. **Finding Number 9** p. 39
Civil agency archives are extensive, uncoordinated and a potentially important source of data for domestic users.

k. **Finding Number 10** p. 40
Need to change reporting procedure for U.S. persons.

l. **Finding Number 11** p. 41
Need for balanced discussion of domestic use of IC capabilities.

Chapter 3: Other Models Considered p. 43

Chapter 4: Next Steps p. 47

(Distributed on CD only)
Appendix I Terms of Reference
Appendix II ISG and SSG Members
Appendix III Study Methodology
Appendix IV The CAC Charter and History
Appendix V ISG Agendas
Appendix VI ISG Briefings to the SSG
Appendix VII Glossary

Classified:
Appendix VIII Briefings given to the ISG
Classified Discussion of Finding #6
(Distributed on a separate CD, by request only; call Mr. Randy Soderholm, ODNI, 703.482.5709 or Marty Eckes, USGS, 703.648.5746.)

Executive Summary

Recognizing a growing need for use of domestic information collected by the Intelligence Community, in May of 2005, the DDNI/Collection and the Director, U.S. Geological Survey, chartered an Independent Study Group (ISG) to review the current operation and future role of the Civil Applications Committee (CAC) and study the current state of Intelligence Community support to homeland security and law enforcement entities.

The ISG concluded there is *an urgent need for action because opportunities to better protect the nation are being missed*. They unanimously agreed on 11 significant findings and 27 recommendations. The ISG found that although the civil domestic users are well supported through the CAC, homeland security and law enforcement users lack a coherent, organized, and focused process to access IC capabilities. Most of these users do not understand how intelligence capabilities can be applied to support their missions and functions. Likewise, the IC lacks a comprehensive understanding of the needs of those users. For these and other reasons, the ISG concluded a new management and process model is needed to effectively employ IC capabilities for domestic uses.

To better support domestic users, the ISG recommends establishment of a Domestic Applications Program, funded by the DNI. Within that program the Department of Homeland Security, as executive agent of the Director of National Intelligence, would house a Domestic Applications Office (DAO) to provide a focal point and act as a facilitator to the IC on behalf of civil, homeland security and law enforcement users. Oversight would be provided by a Domestic Applications Executive Committee composed of elements from the IC and other significant stakeholders. The DAO would be informed by working groups from each of the domestic user domains: civil, homeland security and law enforcement. This process would be modeled after the successful operations of the CAC.

This new management and process model for the domestic users will necessarily evolve overtime. To aid in this *process of discovery*, the ISG also recommends a Domestic Applications of National Capabilities (DANCAP) Program be established to promote greater use and understanding of IC capabilities and their application to solve the needs of the domestic user.

An effective and growing use of IC capabilities for domestic needs will have significant implications for R&D, acquisition and Tasking, Collection, Processing, Exploitation and Dissemination (TCPED). Although the ISG concluded expanded access to current IC collection and processing capabilities by domestic users can be accommodated without major impact, exploitation and dissemination requirements could be extensive and more difficult to accommodate. Today, most domestic users are absent from DNI, IC and DOD requirements and systems development forums. This must be corrected. The ISG recommends the domestic users be given a "seat at the table" to influence policy, R&D and acquisition decisions.

The current lack of understanding between the users and providers concerning domestic information makes imperative a need for training and education. Domestic users need to know

and understand what the IC can and cannot do in supporting their requirements. Conversely, the IC needs to better understand the domestic user's requirements. This can best be addressed through a sustained and comprehensive training and education program, sponsored by the DNI.

The study also found significant change is needed in policy regimes regulating domestic use of IC capabilities. The root of the problem is a lack of a clearly articulated comprehensive policy on the use of IC capabilities for domestic needs. Today, policies and practices governing the use of IC capabilities, many of which pre-date 9/11, discourage rather than encourage use by domestic users especially law enforcement. As a consequence, access is often governed on a case-by-case basis through a risk averse rather than risk management lens. Support to domestic users often appears more like a "pick-up game" rather than a well coordinated, focused and repeatable process, despite commendable efforts by all involved to make the system work. The ultimate effect is missed opportunities to collect, exploit and disseminate domestic information critical to fighting the war on terrorism, preparing for, responding to, and recovering from disasters, natural and man-made. To address these shortfalls, the ISG recommends convening a study to comprehensively review the laws, policies and practices concerning classification of information, limits on information collection, storage and dissemination, and to reconcile the need to use domestic information with the keystone requirement to protect the civil liberties and privacy of US persons.

Finally, the ISG noted other matters that must be addressed:

- Timely and efficient provision of geospatial intelligence support to domestic users is impeded by policy barriers, classification issues and culture; and,
- Effective IC support to federal, state, tribal, local and private sector authorities is complicate by overlapping jurisdictions and barriers to information sharing; and,
- Exploitation, fusion, storage and sharing of "domestic information" is complicated because current rules require extensive special handling protections; and,
- Civil agency archival holdings are extensive, but uncoordinated; and,
- There is a need for change in the procedures for reporting U.S. person data including more rapid transmission of identity in specific threat situations; and,
- A concerted effort to assure a balanced discussion of the benefits and risks associated with expanded use of intelligence capabilities for domestic purposes will be needed.

This report provides the first comprehensive review of the role IC capabilities currently play in supporting domestic information needs of civil, homeland security and law enforcement users since the establishment of the CAC in 1975. The ISG concluded dramatic change is required. This report and the recommendations it makes represent a unique opportunity to better protect the nation.

CHAPTER 1: INTRODUCTION

In late May 2005, the Deputy Director of National Intelligence for Collection and the Director of the United States Geological Survey commissioned Booz Allen Hamilton to lead a Civil Applications Committee (CAC) Blue Ribbon Study. The objective, as stated in the Terms of Reference, was to:

> "Conduct an independent review of the future role of the CAC for the facilitation, management and oversight of remote sensing for applications that are civil and/or domestic in nature and involve the use of Intelligence Community (IC) capabilities and products. This study is predicated upon the realization that many of these applications have taken on increased importance and the CAC construct that was put in place several years ago may no longer be well suited for meeting current and future needs. In addition to applications where the CAC has traditionally been involved, which include natural disaster recovery, environmental applications and support of civil agency special requirements, the study will address management and processes associated with leveraging Intelligence Community capabilities against homeland security and law enforcement missions. Recommendations will be developed to improve the effectiveness, timeliness and efficiency of the Intelligence Community support to civil, homeland security and law enforcement users and will address the future role of the CAC in the process."

The study was conducted by an Independent Study Group (ISG) composed of eight former senior government/military officials and consultants and led by Mr. Keith Hall of Booz Allen Hamilton (see Appendix II for a list of members). The study was conducted under the oversight and guidance of a government Senior Steering Group (SSG) co-chaired by Mrs. Mary Margaret Graham, DDNI for Collection and Dr. Patrick Leahy, Acting Director, USGS (see Appendix II for SSG membership).

Federal civil agency access to classified remote sensing data for scientific purposes was facilitated from the beginning of national technical programs through the involvement of President Eisenhower's Science Adviser, James Killian. Through 1972, the use of national overhead systems data for civil, scientific and environmental purposes was accommodated through the offices 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 in response to Committee opposition to the administration's anti-ballistic missile system initiatives. The lack of federal oversight complicated civil access to classified systems data and products.

In January 1974, 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 a Presidential Commission, chaired by Vice President Rockefeller, to examine CIA operations within the US. One of the Rockefeller Commission's tasks was a review of the entire range of classified overhead remote sensing capabilities targeted at domestic areas. While failing to substantiate any illegal use of classified imagery, the Commission's report noted that the

demise of the PSAC and the Science Adviser positions eliminated oversight authority for managing legitimate civil activities involving access to classified remote sensing resources.[1]

A key Rockefeller Commission recommendation urged establishment of an interagency committee of Federal civil agencies to facilitate appropriate use of overhead remote sensing technology and allay concerns about the potential for improper use of intelligence assets for domestic purposes. The Committee for Civil Applications of Classified Overhead Remotely Sensed Data, also known as the Civil Applications Committee or CAC, was chartered in 1975 through a joint memorandum signed by the Assistant to the President for National Security Affairs, the Director of the Office of Management and Budget, and the Director of Central Intelligence.

The CAC, with membership of 11 departments and independent agencies, is chaired by the Director, U.S. Geological Survey, and meets monthly as a technology and information exchange forum. The CAC has an Executive Steering Group of senior agency officials, chaired by the Deputy Secretary of Interior, who meet biannually to address policy issues of common interest in the DoD, intelligence, and civil communities. In addition, the monthly CAC and the Executive Steering Group are supported by a secretariat hosted by the U.S. Geological Survey. The Secretariat is the principal means of interaction between the civilian agencies and Intelligence and Defense agencies. The CAC provides a means for communication between the civil users of intelligence community capabilities and the providers. Technology developments and novel applications are shared, support for response to hazards is facilitated and the staff of the CAC coordinates training for the civil community. In addition, the CAC oversees requests for information from the civil users to ensure that it conforms to the charter of the CAC and cannot be otherwise obtained in a timely fashion. Technical support for the acquisition, receipt, archiving, and dissemination of data is provided to the CAC through the USGS National Civil Applications Program (NCAP).

The attacks of September 11, 2001 have had a significant impact on the policies, roles, missions and structure of the U. S. government. The need to share information across the government, and between federal, state, tribal and local jurisdictions, is slowly taking hold and the benefits are starting to be realized. With the exception of the Civil Applications Committee effort, Intelligence Community capabilities have traditionally supported national security and foreign policy elements of the government. As noted above, limited resources were devoted to domestic civil agencies support and then only on a low priority, resources available basis. Today, the threats to the Nation have changed and there is growing interest in making available the special capabilities of the Intelligence Community to all parts of the government, to include homeland security and law enforcement entities and on a higher priority basis. The American people expect their government to use all available resources to protect them.

This study considers how the civil, homeland security and law enforcement communities of the United States can access intelligence capabilities while at the same time protecting the civil liberties of U.S. citizens and the sensitive sources and methods of the intelligence community.

[1] In 1976 the position of Science Adviser to the President was reestablished; however, there has never been any reinstitution of the link between the position and the CAC.

Definition of Terms

A short clarification of terms is necessary so that their use will be interpreted in the manner intended by the Study Group. During the study we used the term "Domestic User" to indicate all civil, homeland security and law enforcement domains. The word "Domain" refers to a customer community that might use intelligence capabilities in support of their respective missions. There are three such domains: Civil, Homeland Security, and Law Enforcement.

- The "Civil Domain" (Civil) involves government activities involved in scientific or environmental research to include monitoring and recovery from natural disasters and related hazards. This domain includes the current members of the Civil Applications Committee as well as other relevant elements of the government (e.g., General Services Administration, Department of Health and Human Services, etc.).
- The "Homeland Security Domain" (HLS) encompasses those elements of the government involved in the preparation, prevention, response and recovery to attacks on the homeland. This domain includes the Department of Homeland Security (DHS) and its various subcomponents, and other federal, state, local and tribal elements involved in these activities.
- The "Law Enforcement Domain" (LE) includes Federal, State, Local, and Tribal activities aimed at investigation, arrest and prosecution of criminal activity, including regulatory enforcement.

The use of domain definitions for functions eliminated the organizational complexity of the many roles performed by most government organizations; with many having functions in two or even three domains. For example, the Department of Homeland Security also includes FEMA (which has the Civil Domain responsibility to respond to natural disasters), as well as the Customs and Border Protection element which has a significant homeland security and law enforcement role. The FBI has a long standing law enforcement role, but also has responsibilities for the prevention of terrorist attacks (a homeland security role). The Environmental Protection Agency has an environmental monitoring role in the Civil Domain, but a regulatory enforcement role which for purposes of this study is considered a Law Enforcement role.

Intelligence Capabilities (as used in this report) includes: national satellite sensors; technical collection capabilities (archival, current & future) of the DoD; airborne sensors; NSA worldwide assets; military and other MASINT sensors; and sophisticated exploitation/analytic capabilities.

Factors Affecting Domestic Use of Intelligence Capabilities

During the conduct of the study, it became clear that there are several factors that currently affect the domestic use of intelligence capabilities. This group of factors has both limiting and facilitating impacts on a customer's access to IC capabilities. First is the degree of familiarity with IC capabilities. CAC members over thirty years have developed an extensive knowledge of IC capabilities and therefore are successful in using those capabilities to support their requirements. The law enforcement domain is at the opposite end of the spectrum. They are for

the most part unfamiliar with the IC's capabilities and the type of support they could obtain. The knowledge of the homeland security domain is evolving as DHS matures. Awareness of the IC's capabilities is a major factor in gaining support.

Second, the availability of a means for accessing IC capabilities varies greatly. For 30 years the civil domain has used and improved the CAC process. It is well established, known in the IC and civil communities and has been successful in providing support. DHS has access by virtue of its membership in the IC and the CAC. While the law enforcement domain, in theory, has access via DHS and FBI, it is clear these access paths do not have an established process, and where paths do exist, they are not widely known within their domains. Therefore, support is minimal to the LE domain but improving in the case of the homeland security domain.

Third, there is a wide misperception that domestic information collection requests cannot compete with foreign collection priorities and therefore will be given a low priority and take months to satisfy if at all. The consequence in most cases is customers are discouraged from trying to access information that may be valuable to them. The reality is although many domestic collection requests do not impinge on foreign collection requirements, exploitation and dissemination capabilities may indeed be impacted. The lesson is clear: knowledge of IC capabilities improves access and support.

Fourth, the extent to which domestic users have established relationships with IC agencies has a positive impact on their ability to get domestic support. In particular, those agencies served with an IC agency liaison officer are more likely to receive valuable support from the IC. Support by NGA and NSA to the Department of Homeland Security has been particularly aided by the presence of liaison officers at DHS.

Fifth, the problems associated with handling different classification levels and categories of information impacts support. Even though a few State and local officials are being given security clearances and more and more information is being sanitized for release at the unclassified level, access and storage is a continuing and growing barrier to information flow. Related to this issue is the degree of interoperability and connectivity between federal, state and local communities. There is no single system that allows information to flow quickly between these entities. Therefore, even if the information is available at an appropriate classification level, there may not be a fast, convenient communications network available to get the information to the user in time.

Sixth, decisions are made and policies written regarding access and use of information and capabilities of the IC using a risk avoidance vice a risk management philosophy unnecessarily restricting the uses of domestic information. Further, requests of the IC for domestic information are treated as an exception to the rule and as such, cause a slow bureaucratic process to carefully ensure there is no compromise of the system, its' capabilities or the civil liberties of U.S. citizens. The process sets unnecessarily high standards for most domestic requests. In the case of law enforcement domain support, in addition to the barriers described, a further barrier is imposed regarding protection of sources and methods. Since prosecution is the principal purpose of most law enforcement activities, the potential for information being made public during the

discovery process and trial, contributes to the reluctance of the IC to support the law enforcement domain.

Finally, the limited availability and capacity of exploitation/analytic resources inside and outside the IC impacts the ability of domestic customers to get their requests satisfied. The ability to exploit information is much more limited than the ability to collect it. Many customers do not request information because they can't exploit the data themselves or they can't find someone else to exploit it for them. This in no way degrades their need for the data. This is an age-old problem that the IC continues to struggle with. There is no easy answer. However, now that "National Intelligence"[2] includes information gathered within or outside the United States irrespective of the source from which it is derived, the playing field should be level when it comes to establishing relative priorities for domestic requirements.

CHAPTER 2: FINDINGS AND RECOMMENDATIONS

The ISG developed 11 findings, if acted upon, will make dramatic improvements in the process to use IC capabilities in support of domestic applications and in the security of the Nation. The following chapter outlines the problems encountered and explains the ISG's solutions.

During the course of the study, no one said that they were failing at their mission due to the lack of access to IC capabilities. There was no "Burning Bridge" identified by the participating agencies and stakeholders. However, there were many areas where the process was shown to be broken and where efficiencies in the process can be realized to greatly increase the timeliness and relevance of the information provided. The current system operates in a risk-averse vice risk-management environment where protection of sources and methods and individual civil liberties, while important concerns to be carefully considered and taken into account, are the predominant concerns unreasonably operating to limit appropriate support to the defense of the homeland. Dedicated government employees are finding ways around the system to support the civil, homeland security and law enforcement communities. Such work-arounds are confusing, usually a "one off" process and at best delay support and at worst, prevent support. The process should not be that hard when it comes to supporting the defense of a nation that is involved in a global war on terrorism.

Finding #1:

- ***At present, HLS and LE users lack a coherent, organized, efficient process to access IC capabilities. As a result, opportunities to provide critical support are being missed***

[2] "…The terms 'national intelligence' and 'intelligence related to national security' refer to all intelligence, regardless of the source from which derived and including information gathered within or outside the United States, that- (A) pertains, as determined consistent with any guidance issued by the President, to more than one United States Government agency; and (B) that involves- (i) threats to the United States, it's people, property, or interests; (ii) the development, proliferation, or use of weapons of mass destruction; or (iii) any other matter bearing on United States national or homeland security." Pub. L. 108-458, Sect. 1012, Dec., 17, 2004.

***Recommendation*:**

- ***Establish a Domestic Applications Office (DAO) employing a "CAC Like" process with the Department of Homeland Security as Executive Agent for access to Intelligence Capabilities by Civil, HLS and LE users.***

***Discussion*:**

The ISG noted a number of reasons prompting this finding:

- Until 9/11 the role of law enforcement was almost completely focused on arrest and prosecution.
- The use of NTM and other US intelligence assets was and is not well understood by the LE community.
- The IC and the LE domain were and to some extent, still are separated by legal boundaries, cultural differences and operational priorities.
- The IC has been wary of involvement with LE because of the role.
- discovery plays in prosecution and the possibility that sources and methods could be compromised.

During the past 30 years, most civil requirements for access to NTM were met through the Civil Applications Committee (CAC) process. The CAC charter did not extend, however, to LE and for the most part, any local or state LE requests for use of and information from NTM and, indeed, from the IC have been handled through a single conduit, the FBI: specifically the Joint Terrorism Task Force (JTTF). As a result of issues identified by US Government, US Government sponsored and independent studies, as well as perceived cultural differences between the FBI and State and local LE, DHS was created to help foster better relations between all facets of LE and the IC, as well as to facilitate the collection and movement of terrorism-related intelligence and information in ways not previously considered pre 9/11. Regardless of the intended unifying role of DHS, redundant responsibilities for the collection, analysis and dissemination of intelligence to and from LE are a troubling reality and competition for authority and assets has resulted in a less than ideal situation.

The DNI must take the lead in pulling together the relevant agencies and other entities to bring expertise and solutions to the problem. All persons involved in this endeavor must be from the senior leadership of the relevant agencies to ensure that the results are implemented and receive the highest support. Engage and advise the Executive Branch and Congress in addressing and solving problems related to overlapping authority, funding and clarification of responsibilities as well as the legal issues associated with interfacing IC and LE assets, capabilities and the 2-way flow of information, data and analytical product. It is imperative that redundancy of authority be dealt with. If not, the existing situation and the problems it causes, (dilution of funding and resources, energy wasted on turf battles, confusion and disconnection in information and intelligence sharing), will negate any improvements.

Information sharing and access to relevant data must include State and local entities such as fire and medical. 95% of US infrastructure is in the hands of the private sector and any consideration of constructing an architecture to move information and data needs to consider these realities.

Develop a training and awareness program to broaden understanding of capabilities, share available information, and foster an atmosphere of trust and teamwork is vital to a successful process. The following elements are essential to this program:

- Identify and instruct all members of LE as to the usefulness and relevance of IC capabilities to their new mission vis-à-vis the war on terrorism.
- Educate the IC and LE as to the standards relating to sharing information and capabilities as well as promoting understanding mission focus. The results from training LE in basic tradecraft have been very positive and successful. LE has traditionally focused on arrest and prosecution and the IC on disruption and prevention. These mission foci are blurring and common training can be extremely helpful in making this a "feature" as opposed to a "flaw".
- Foster a "purple" culture among members of the IC and LE. Trust has always been and will remain the basis of constructive relationships and common training and experience promotes and nurtures this bonding.
- Identify a successful model or models that LE can use to better integrate with the IC. The LAPD ATD/MCD, (Anti-Terrorist Division/Major Crimes Division) model is one example where these departments have been doing intelligence analysis for over 30 years and are modeled after the CIA. For interaction between the IC and LE, the CAC model stands out because of its experience and successful track record. This is a goal of the Law Enforcement Working Group (LEWG). Further consideration should be given to having the CAC be a part of DHS, especially as DHS is unique in its legal authority to connect State and local with Federal assets regarding matters of homeland security and terrorism.

There are now a number of members of the LE who are cleared at the SCI level and above and, combined with training in and exposure to the capabilities and analytical skills once residing only in the IC, they could make a real contribution to the overall US capability by applying analytical skills to regional and local situations, creating a cadre of IC-capable analysts giving depth to US analytical capabilities, providing a surge capability in a situation where international priorities stress the IC community and finally, being able to inject knowledgeable people immediately into the IC/LE mainstream.

Most people would agree that the best intelligence from a given area would come from those most familiar with that area and it is imperative that those members of LE and the first responder community have the skills to receive and create relevant intelligence from inside our national borders. It is not an easy task, especially because it must be done with consideration for privacy and preservation of personal and national freedoms. As we examine and implement new methods and relationships for doing intelligence, we have the opportunity to consider and codify the necessary safeguards to promote the trust and participation of all parties, vital to the success of any implementation of modernizing, improving and adapting a new intelligence paradigm.

In light of this recommendation, the ISG considered 5 different process models that arguably could address the issues identified and improve the status quo. Most of the models considered would work given appropriate domain experts at key points in the process and detailed guidance on procedures and boundaries was available. The challenge was to find a process that could support a diverse set of customers, keep bureaucracy to a minimum, be sustainable and be easy to use. The ISG evaluated the models against the following thirteen characteristics of an effective process:

- Ensures an opportunity for access to the full range of civil, homeland security and law enforcement users
- Creates a culture where information sharing is the rule, not the exception
- Supports routine, ad hoc and crisis requirements
- Ensures visibility, flexibility and ease of use
- Assures timely legal and policy adjudication
- Processes "sensitive" requirements discreetly
- Delegates decision making authority to the lowest level
- Domain experts are at critical points throughout the process
- Provides efficient, effective and sustained infrastructure support
- Provides clear delineation of budgetary authority
- Leverages exploitation, product generation and dissemination capabilities
- Promotes interoperability through two-way training and standardization (within the IC and Domestic communities)
- Uses metrics to monitor performance and improve the system

With these characteristics in mind the ISG then developed the following factors used in deciding on the recommended process model:

- Do no harm
- Positive public perception
- Ease of transition
- Budget sustainment
- Opportunity for user access
- Protection of civil liberties
- Protection of sources and methods
- Community wide education and training process
- Low degree of process complexity
- Ability to foster cross-fertilization

The Model:

In deciding on a process model, the ISG realized what they are recommending is the first step in a "Process of Discovery". Time and operational experience will evolve the model into the most effective, efficient and sustainable program.

After extensive discussion of the benefits and limitations of five models, the ISG decided on a process model that employs a centralized broker situated outside what is "generally perceived" as the Intelligence Community. (**Figure 1**) They also agreed that the Director of National Intelligence was best suited to be the overall owner of the program. The centralized broker model was chosen because it encourages a multi-INT solution to requests; it has the ability to leverage all of the IC's capabilities; it provides a single consistent process; and the requestor does not need to have a detailed knowledge of the IC and it's capabilities to acquire information.

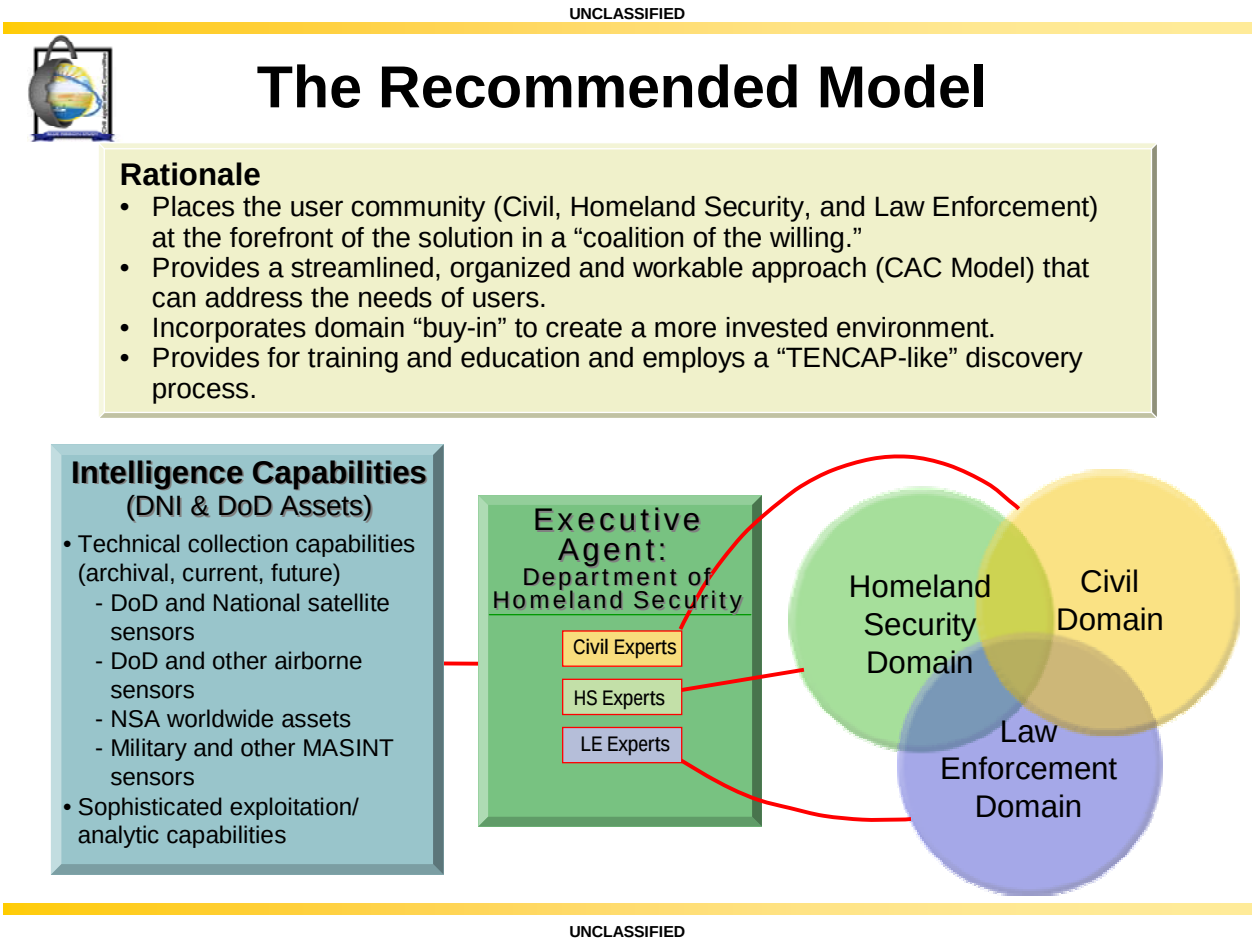

Figure 1. Domestic Applications Program Process Model

***Governance*:**

The DNI, as the owner of the Domestic Applications Program (DAP) and the principle provider of national technical capabilities, should ensure funding, provide oversight and a community training and education program for the DAP. (**Figure 2**.)

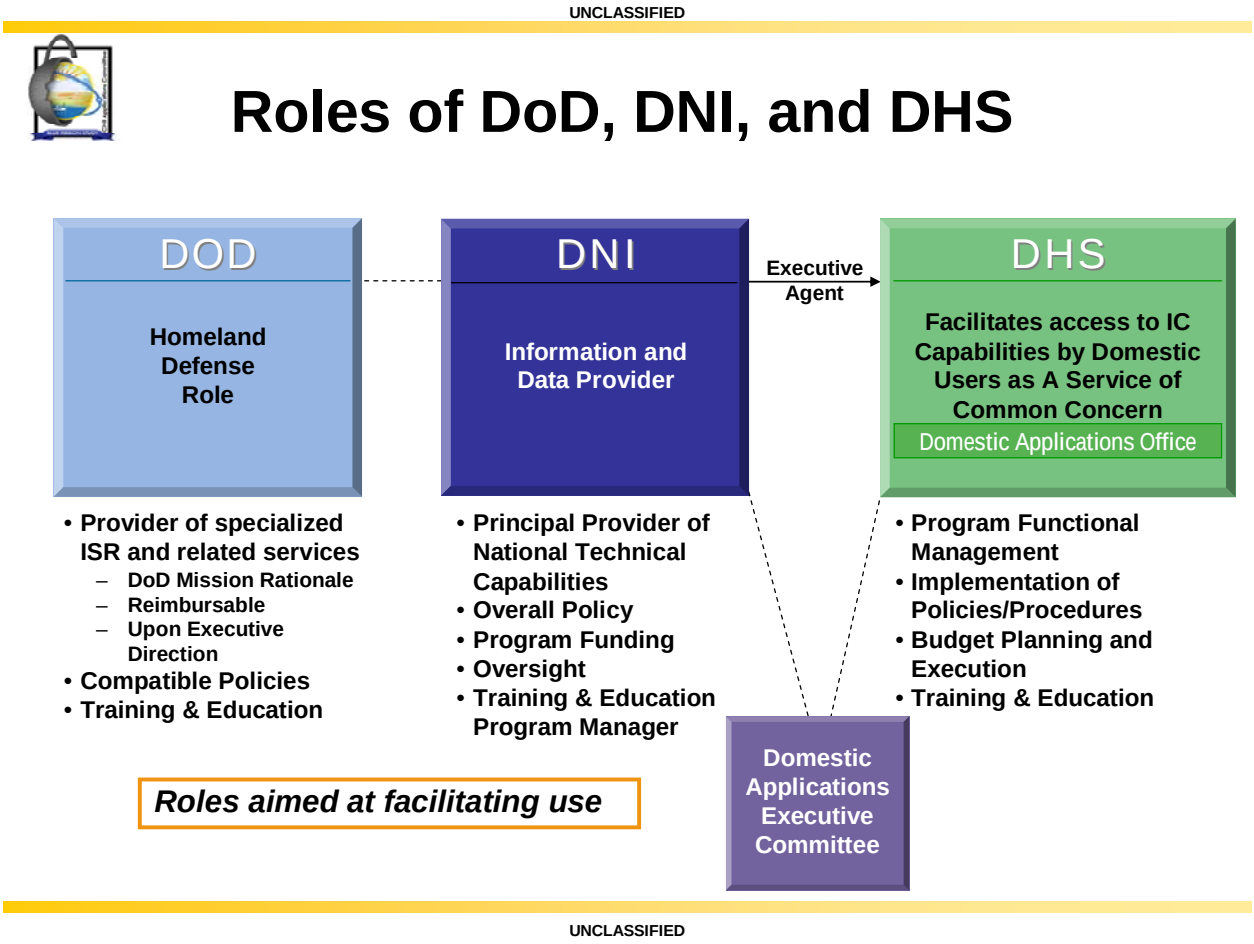

Figure 2. Top Level View of Model

An "Executive Agent" construct is proposed to ensure a clear line of program authority and an unambiguous budget process. The ISG felt that an identifiable budget program was required to ensure that the domestic access process would be sustained and improved over time. The ISG believes that this process is best implemented as part of the Department of Homeland Security, which is uniquely situated, to look across the entire National Intelligence process (foreign and domestic) and has extensive ties from the cabinet level right down to the local government level.

The ISG recommends that the DNI reach an agreement with the Secretary of the Department of Homeland Security to establish and define the "Executive Agent" for Domestic Applications of IC capabilities. The Secretary of DHS would provide a service of common concern for the government and as the Domestic Applications Program Functional Manager, be responsible for budget planning and execution, training and education, and implementing domestic policies and procedure. The ISG specifically recommends the Executive Agency model to ensure that DHS has: authority to lead, coordinate and integrate the domestic uses of IC capabilities; budgetary responsibility to include recommending planning and programming guidance and to be the proponent for the civil, homeland security and law enforcement communities in the IC requirements development and acquisition process.

To help the DNI and the Secretary of DHS administer this process, we recommend the establishment of a Domestic Applications Executive Committee (**Figures 2 & 3**). This group would be co-chaired by the Director of National Intelligence and the Secretary of the Department of Homeland Security. I would be a community forum of producers and consumers to advise the DNI and DHS, monitor and advocate the program, be an initial multi-agency program funding resolution forum and foster cross-fertilization and innovation in the application of IC capabilities to solving domestic problems. The Committee would be composed of representatives from the National Security Agency, the National Geospatial-Intelligence Agency, the National Reconnaissance Office, the Department of Defense, the Department of Justice, the Federal Bureau of Investigations, the Department of Interior, the Civil Domain Working Group chairman, the Homeland Security Domain Working Group chairman and the Law Enforcement Domain Working Group chairman. The co-chairs could have advisors (such as the DNI Civil Liberties Protection Officer and the DNI General Counsel, to assist the committee as they choose.

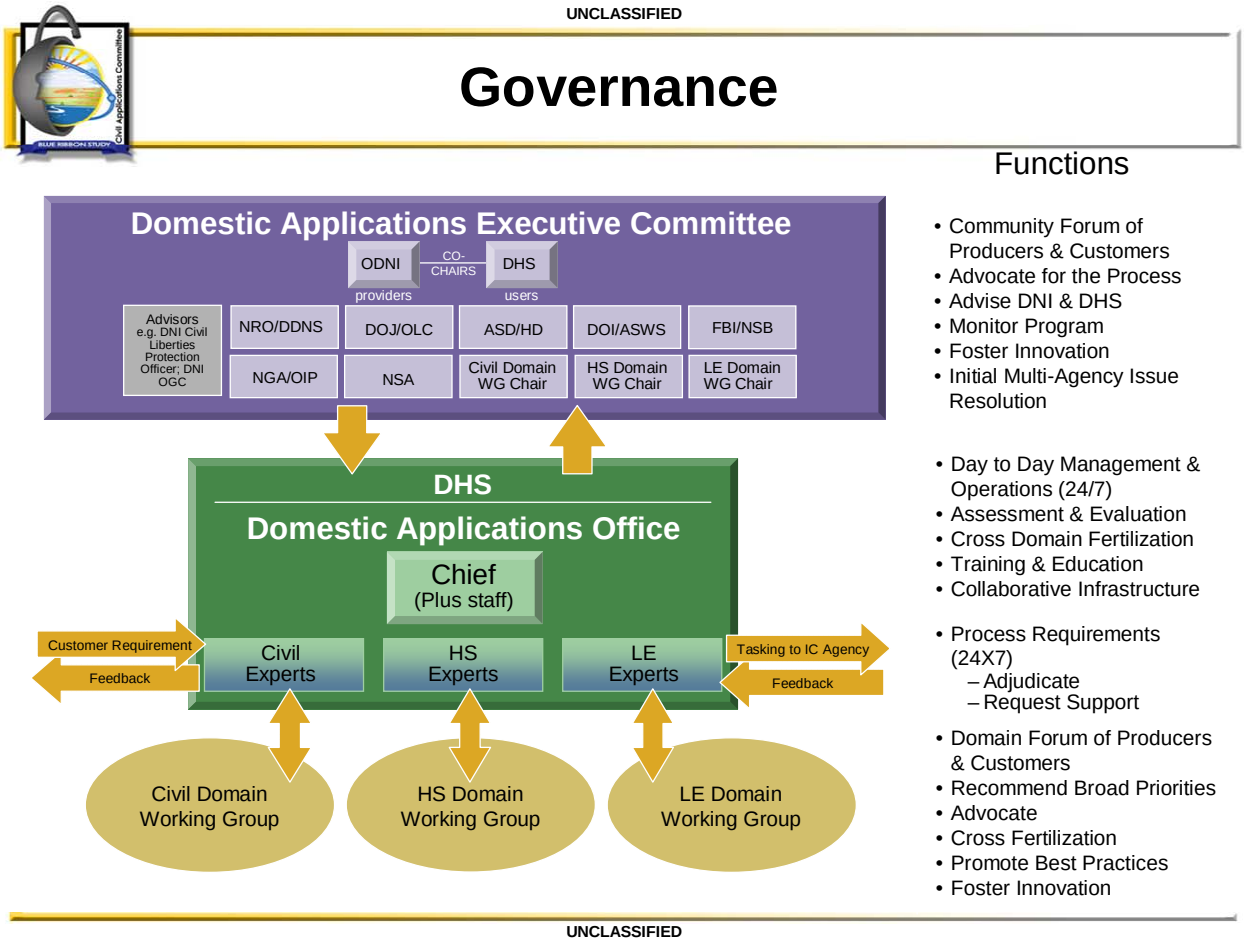

Figure 3. Governance Process for Model

Within the Department of Homeland Security we recommend the creation of the Domestic Applications Office (DAO). Charged with the day-to-day operations of the program, this office would be composed of at least a Chief, a deputy, an administrative support staff, a budget officer,

a legal advisor and several civil, homeland security and law enforcement domain experts to process requirements. Staffing and resources for this office would not come out of DHS resources, rather would be resourced by the DNI. It would be the heart of the program with the domain experts responsible for the day-to-day adjudication of requirements and the integration and cross-fertilization of ideas (**Figure 3**). The DHS over time would have to determine if this function is needed on a 24/7 bases. Finally, the office would provide support to the Domestic Applications Executive Committee.

Advising the Domestic Applications Office would be the civil, homeland security and law enforcement domain working groups. These domain forums of producers and users would advocate the use of IC capabilities, foster cross-fertilization of ideas and techniques, promote best practices, recommend broad domain priorities to the DAO and foster the innovation of new experimental uses for IC capabilities through a "TENCAP" like program. Primary membership would be domain specific and include the DAO domain experts. However, attendance by representatives from other domains should be encouraged to improve cross-fertilization (**Figure 4**).

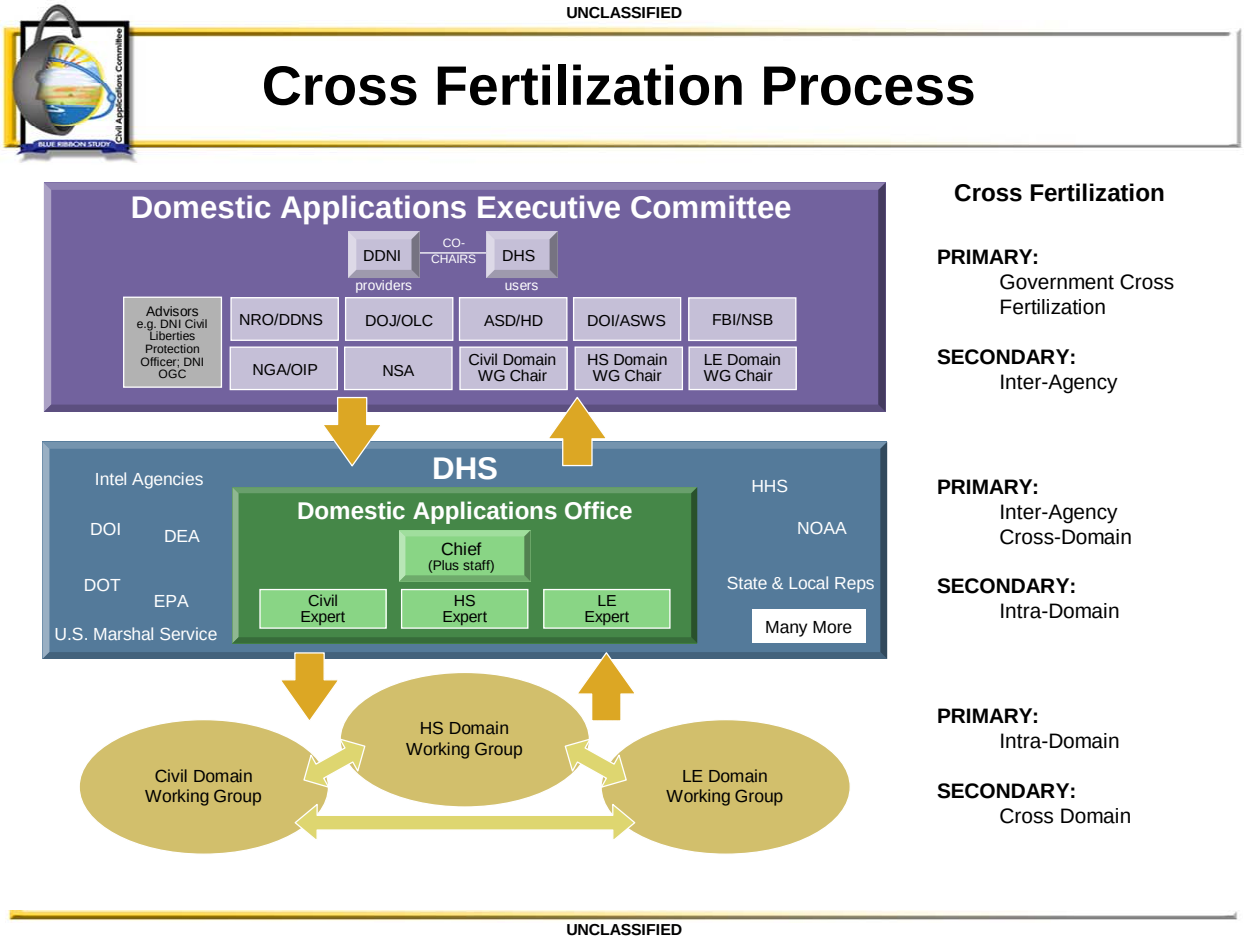

Figure 4. Model Cross Fertilization Process

DHS should take advantage of existing facilities and experts in the USGS Advance System Center (ASC) to help those agencies who lack the secure facilities or equipment to process, exploit and publish classified data. DHS, in conjunction with the Department of Interior, should designate the ASC as a service of common concern for the domestic user community. As well as facilitating current programs, the center could act as a focal point for innovative applications of IC capabilities.

***Policy and Legal*:**

At the core of IC support to the domestic community is clear, timely legal and policy documentation and decisions. Currently, the environment is one of risk avoidance vice risk management. Although there has been some effort to update policies since 9/11, the ISG noted some significant policies and corresponding documents do not or inadequately take into account the threat to the U.S. homeland. The legal regime governing the use of IC capabilities domestically is unsettled, due to a number of factors to include the lack of case law compounded by a slow, laborious process to acquire definitive legal positions. The ISG believes a timely, responsive legal and policy guidance process must be put in place to permit the Model to function optimally. The Department of Justice in coordination with the General Counsels of the DNI, DOD and DHS, should establish a "fast track" process to provide for the timely adjudication of domestic legal issues. The DHS/DAO legal advisor would have the authority to raise issues to this group for the community. (**Figure 5**.)

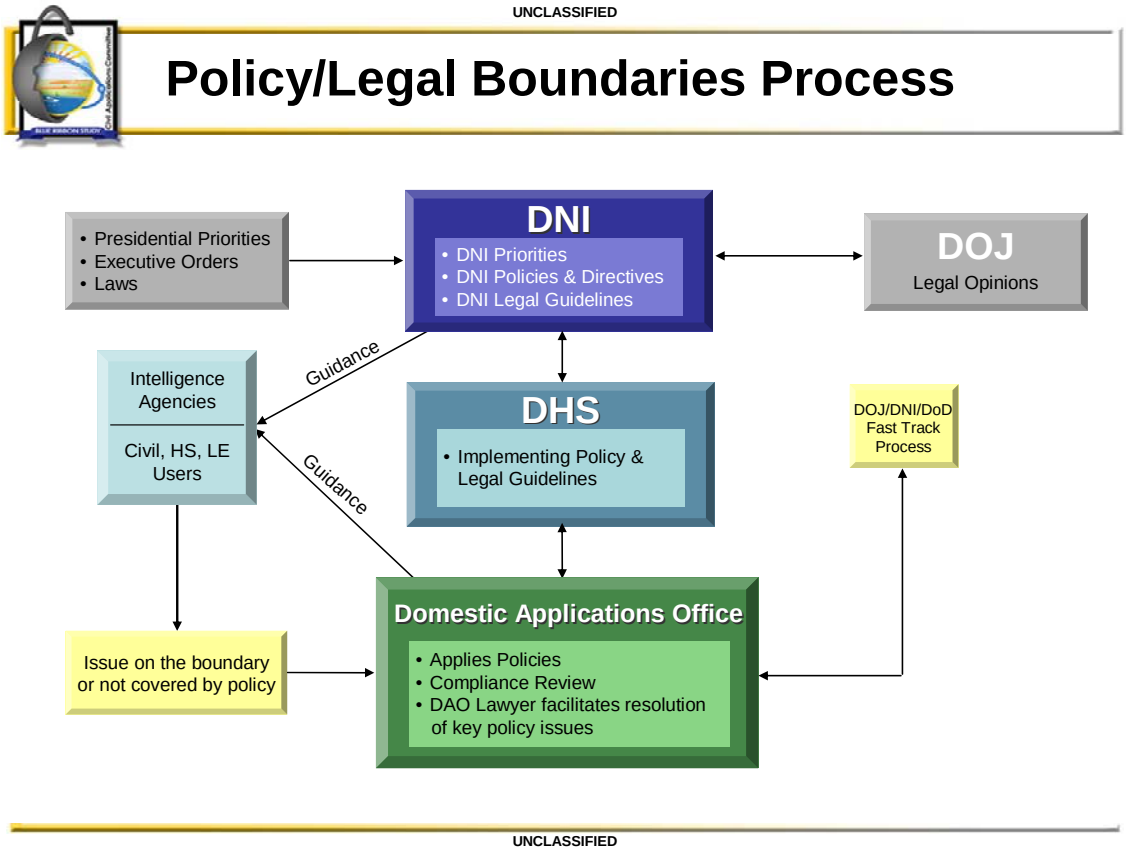

Figure 5. Policy and Legal Process for the Model

The use of IC capabilities for domestic purposes should be governed by a set of guidelines that collectors, producers and users of IC capabilities can easily understand and based on the premise that most uses of IC capabilities are lawful rather than treating *any use* as an exception to the rule requiring a case-by-case adjudication.

***Requirements Flow*:**

The ISG vision for IC support to the domestic community is based on the concept of risk management, a set of clear legal and policy guidelines to operate within and the concept that sharing is possible and necessary in order to maintain the security of the United States. The requirements flow is designed to be simple, flexible and responsive (**Figure 6**). A statement of need would come to the DAO domain adjudication expert via phone, fax or e-mail. The adjudication officer would discuss the requirement with the customer and get a good sense of the requirement and determine if it is possible for IC capabilities to help; at a high level, if the requirement is within policy and legal guidelines and what priority the customer gives the requirement. The adjudication officer would then make a decision as to which agency or agencies are best suited to support the request and forward the requirement to the supporting agency(s) for production.

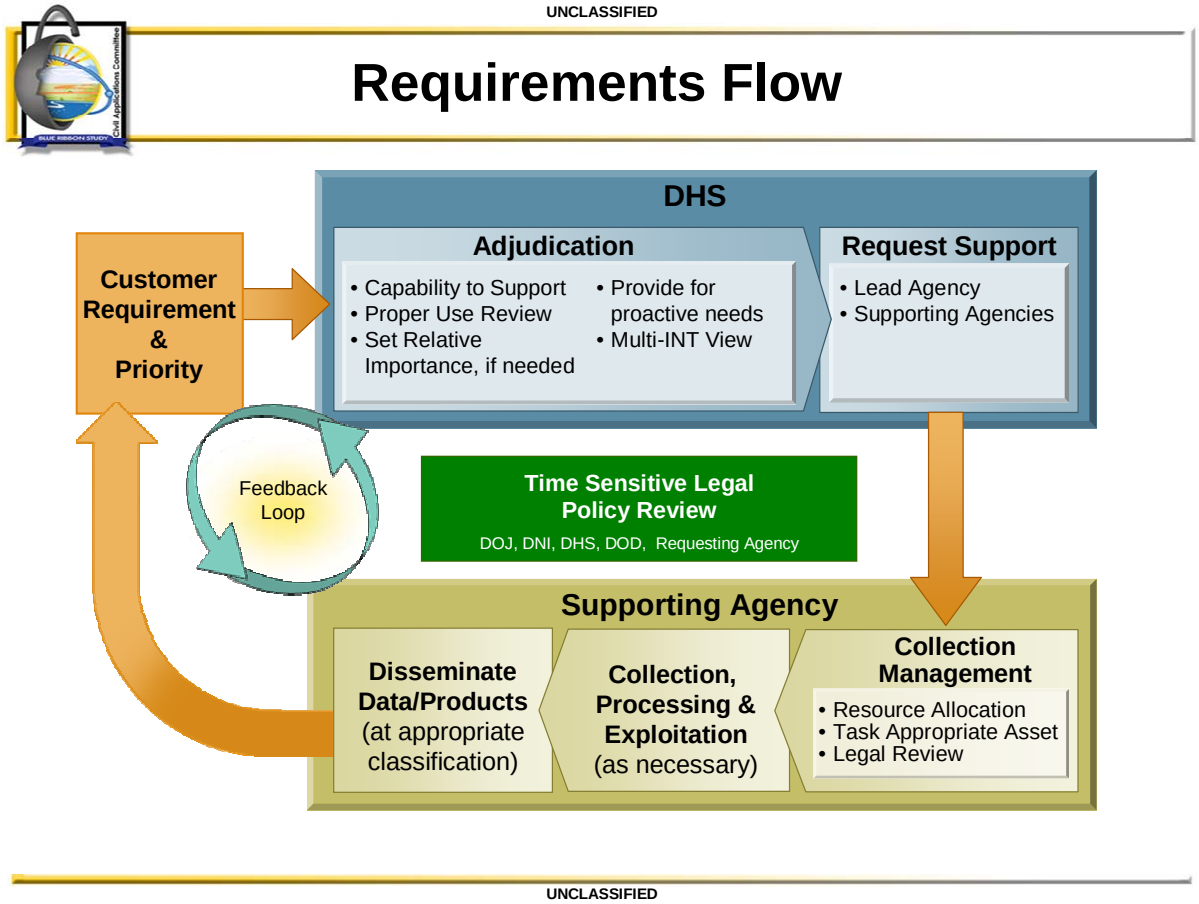

Figure 6. Requirements Flow Process for the Model

The supporting agency(s) would take the request and through discussions with the customer agree upon the information/data required and a completion date. Throughout this whole process there is continuous feedback between the customer, the producer and the DAO as to the status of the project and deliverables. Once the product is produced, it is disseminated to the customer and an information copy is sent to the DAO to ensure awareness. With this in mind, let's look at how a requirement from each of the three domains would be processed in the new environment.

In the civil domain a requirement would be sent from the customer to the civil domain expert in the Department of Homeland Security/Domestic Applications Office (DHS/DAO) for adjudication. For the civil example, let's say the requirement is to image damage caused by a hurricane, to image the everglades to monitor water levels and to monitor glacier movements in Alaska. The officer would discuss the requirement with the customer and get a good sense of the requirement and determine if it is possible for IC capabilities to help; if the requirement is within policy and legal guidelines and what priority the customer gives the requirement.

In this new environment, legal and policy guidelines have been pre-established which foster the use and sharing of domestic information. These guidelines are widely available to all collectors, producers and users of domestic information. Each agency and individual has the responsibility to be aware of the policies and to follow them. The DNI will maintain oversight responsibility and appoint an officer with responsibility for Domestic Applications compliance. Imaging of the United States, by government satellites, for purpose other than specific law or regulatory enforcement, is permitted without case-by-case review and approval. Law enforcement and regulatory enforcement will have much more stringent rules to ensure civil liberties are not abused. The civil example is clearly within the established guidelines.

To help the civil domain adjudication officer establish a first cut at the priority of the requirement, the Civil Domain Working Group has the responsibility on a yearly bases to develop a domain approved list of relative priorities for civil requirements. After discussions with the requester and consulting the civil priorities list, the civil adjudication officer makes a priority recommendation. This process is an effort to ameliorate the common customer belief that "my requirement is very important and therefore a priority one". Not all requirements can be priority one.

Next the adjudication officer reviews the requirement to determine what agency or agencies are best suited to satisfy the customer's needs. They then pass the requirement to the collection and production agency or agencies clearly identifying the lead agency that has responsibility to produce the final product. The production agency calls the requestor to ensure that they understand the requirement, the type of data required and agree upon a completion dated based on the priority, the producing agency's workload and the customer's need for the information. Throughout this whole process there is a continuous feedback process to ensure that the customer, the supporting agency and the DAO are all aware of the status of the requirement. The DAO will keep metrics to aid in resources justifications, improve system performance, and perform customer segmentation analysis. Once the product is produced it is disseminated to the customer, an info copy is sent to the DAO and finally it is stored in the database archives for the community to access if they have the need to know and are properly cleared.

In the homeland security domain a requirement would be sent from the customer to the homeland security domain expert in the Department of Homeland Security/Domestic Applications Office (DHS/DAO) for adjudication. For the homeland security example, let's say the requirement is to use all IC technical capabilities over a remote area of Minnesota where officials have reason to believe a possible radical group is training for an attack on a federal government office building. The request is for immediate collection and exploitation of the data to monitor activity at the farm. Information indicates the attacks are to take place within two months. The officer would discuss the requirement with the customer and get a good sense of the requirement and determine what IC capabilities can help; if the requirement is within established policy and legal guidelines and what priority the customer gives the requirement.

In this case, the homeland security domain adjudication officer raises a red flag when the customer requests to use all IC technical capabilities available to monitor the ranch. The requirement does not meet the current legal guidelines for support so he/she requests guidance from the DAO legal advisor. The DAO legal advisor concludes that the request was not clearly within the current guidelines and immediately calls DOJ for guidance. The DOJ would convene a meeting with the DNI General Counsel, DoD General Counsel and relevant Agency General Counsels to address the issue. This group would expeditiously make a decision and the DOJ would issue a legal opinion on the request.

If the request were denied due to the legal restrictions the request would stop. If it was approved or partially approved the requirement would continue through the process. As this is a time sensitive request, the adjudication officer would immediately call the collection/production agency and task the requirement. Paperwork would be accomplished when time permitted. The collection/ production agency would contact the requestor and discuss the details of the requirement and set in place a process for immediate collection, exploitation and dissemination of the data. Status updates are conveyed routinely between the requestor, DAO and the supporting agency. Due to the sensitivity of the information, dissemination is made only to the customer and DAO.

The IC and domestic user communities need to integrate current existing restricted data base archives to ensure that domestic information collected and produced is available to those with a need to know but restricted from the general user community.

In the law enforcement domain a requirement would be sent from the customer to the law enforcement domain expert in the Department of Homeland Security/Domestic Applications Office (DHS/DAO) for adjudication. For the law enforcement scenario, a group of individuals are staying in a home with very limited access and visibility from the streets. Law enforcement units are ready to arrest the group and need better information about the house and the surrounding area to ensure the operation is successful and the potential for loss of life is reduces as much as possible. The requirement is "highly sensitive" and the police want only necessary individuals aware of the operation. A strict set of legal and protection of civil liberties guidelines would be followed. If it were determined by the DAO legal advisor to be appropriate, the requirement would proceed.

In this case, in order to maintain operational security, the concept of "trusted agents" would be used. Law enforcement officials would call the law enforcement domain expert in the DAO. This person would be a "trusted agent". The officer would discuss the requirement with the customer and get a good sense of the requirement and determine what IC capabilities can help; if the requirement is within established policy and legal guidelines and what priority the customer gives the requirement.

Because this is a "highly sensitive" operation, only the law enforcement adjudication officer and the DAO legal advisor would be aware of the specifics. No specific details would be available in the normal reporting channels. The DAO "trusted agent" would call directly to a "trusted agent" in the supporting agency. Details of the requirement would be discussed and the production agency POC would be put in direct contact with the requestor. From here on out only the requestor and the producing agency POC would be aware of the specific details of the requirement. DAO would be kept informed as to the status only. The objective of a "Sensitive" requirement is keep to a minimum the numbers of people who are aware of specific details and ensure that all the information is keep in data bases not accessible by the general user.

***Metrics*:**

Throughout this process, it is important for the DAO to maintain a set of metrics to be able to judge the effectiveness of the effort, understand where the system can be improved and aid the community in budget justifications. The process should not be overly cumbersome or maintain statistics just because it can be done. The process should focus on who the customers are, the volume of requests, the types of information needed and when there was a short fall in support capabilities.

***The Budget Authority*:**

Critical to the success of the program is the ability to have a healthy, sustained budget for the DAO. As indicated earlier, the DNI is the owner of the Domestic Applications Program. In addition, he/she provides national collection capabilities; some exploitation services (based on volume and priorities), pays the cost of the DAO and has oversight of the program. The Secretary of the Department of Homeland Security is the Program Functional Manager with oversight of the total U.S. government domestic applications program and the responsibility to advocate for the community any new requests for resources. Once new resources are obtained they become part of the operational agencies budget.

The ISG believes that the creation of a Domestic Applications of National Capabilities Program (DANCAP), modeled after the "TENCAP" program, for the domestic community is vital to help insinuate domestic applications in the domains and ensure future evolution and development of systems and procedures and techniques. (**Figure 7.)** The purpose of DANCAP is to foster new and innovative ideas for the use of IC capabilities in solving civil, homeland security and law enforcement domain problems. This program would be initially funded by the DNI and executed by the DHS/DAO. Over a period of 10 years the program dollars would be reduced at the DNI

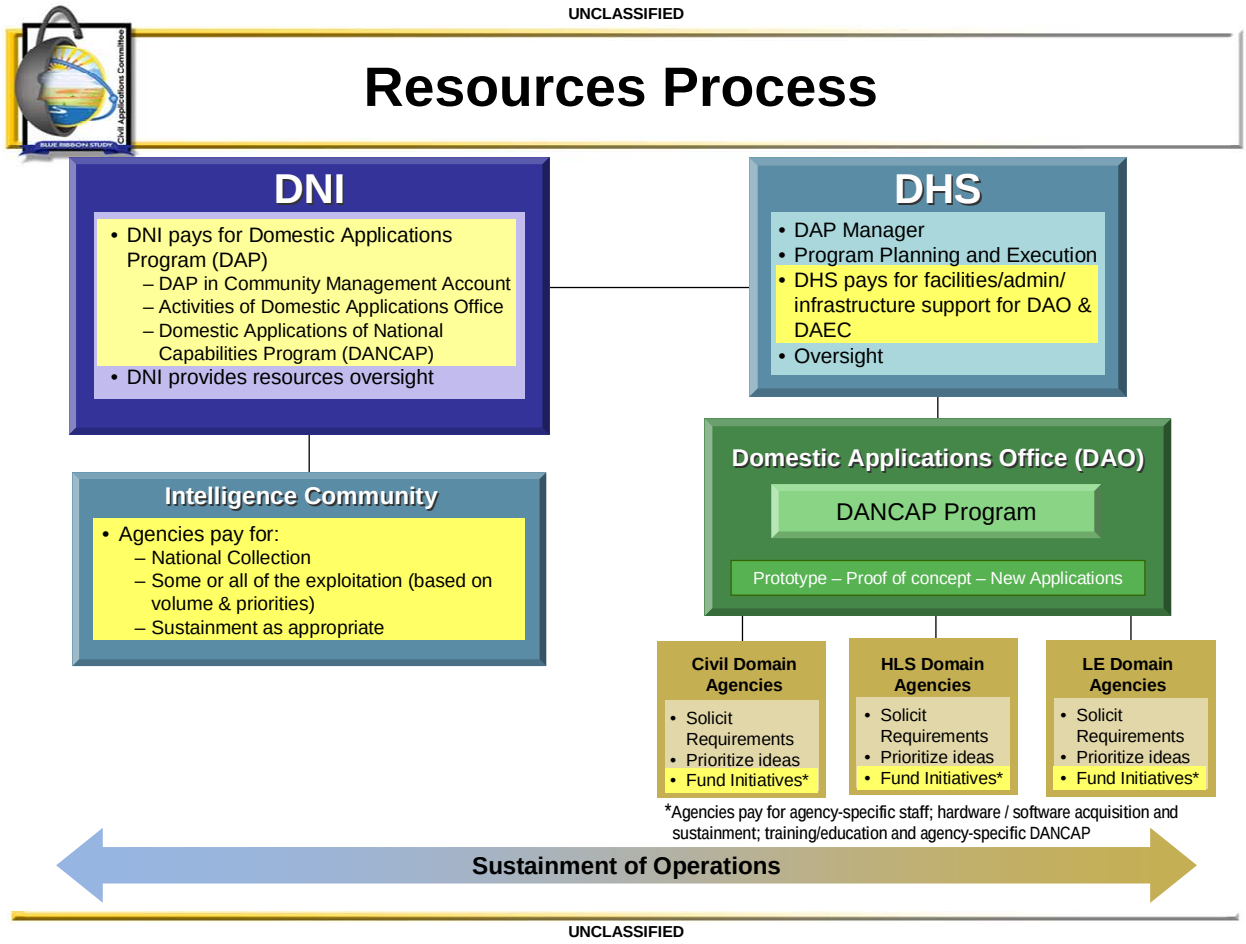

Figure 7. Resources Process for the Model

level and increased at the execution/Agency level and sustained at the Agency level thereafter. An agency in each Domain would be appointed as the focal point for the program. The ISG recommends that DHS be the lead for the homeland security domain, the FBI be the lead for the law enforcement domain and that DOI be the lead for the civil domain.

The DAO would be responsible for the administration of DANCAP. Each year it would solicit candidate projects from the three domain focal points and select the winners. The domain focal points would be responsible for soliciting ideas from their domain, prioritizing them and monitoring the funding of successful ideas in their domain. They would also be responsible for moving successful prototypes to an operational status.

Training and Education:

An initial finding of the ISG was the clear need for a training and education program in the domestic domains and the Intelligence Community. There are three reasons why the domestic community does not use the capabilities of the IC: first they don't know what exists, second, they

don't know how to request support and finally, a very high policy and legal hurdle has to be overcome to achieve support. An extensive education program will help the users understand what is possible and the producers understand what users need and why they need it. The U. S. Marshals Service is a good case in point. If you asked anyone in the IC right now to provide support to the Marshal Service the answer would most likely be a quick "NO". They are law enforcement and we can't do it because of the protection of sources and methods and the slippery slope of discovery. However, a careful analysis of the matter would compel a different result. One of the primary jobs of the Marshals Service is to execute Federal warrants by apprehending people that have evaded the U.S. legal system. This situation presents a very low probability the IC's involvement would be subject to a judicial proceeding. Generally, there should be no problem for the IC to support this type of activity.

A coordinated training and education program lead by the Office of the DNI and executed at all levels of the domestic community can go a long way to resolving this problem. It must be a community effort that is focused on intelligence discipline integration and multi-INT solutions not on individual agency or intelligence discipline's capabilities. The DNI should have overall responsibility for the program. Each Functional Manager clearly has the expertise and operational examples to facilitate training, but only through DNI leadership can a Community program be effective. The DNI needs to work closely with the DOD to ensure that DOD has not only the standard training materials but can adapt these materials to the unique needs of military units.

The ISG believes that the model selected provides a clear entry point and process for all domestic users; a clear funding responsibility and stream of money; organizational sponsorship for the program; domain experts to facilitate requirements; and has the necessary protections for individual civil liberties and sources and methods, all operating in an environment of information sharing vice one of risk avoidance. This process establishes the foundation for the government to effectively use IC capabilities to support domestic requirements.

Finding #2:

- ***The CAC has provided an efficient and effective means to meet civil users' needs and should serve as a model for other domain processes and procedures***.

***Recommendations*:**

a. The CAC's experience and expertise should form the basis for standup of the DAO.

b. The DNI oversee the establishment of a training and education program to ensure domestic users of IC capabilities are aware of the capabilities, security guidelines, examples of uses and the process to access these capabilities. (Build on the CAC success in training)

Discussion:

In 1975, as the result of a Church Commission recommendation, the Civil Applications Committee was formed. The charter of the Committee provides that it is to "facilitate the appropriate civil uses of overhead remote sensing technology and data collected by classified military and intelligence overhead systems and provide to Federal civil agencies". The committee is composed of 11 federal civil departments and independent agencies. The CAC is chaired by the Director, U.S. Geological Survey, and meets monthly as a technology and information exchange forum. An Executive Steering Group of senior government agency officials, chaired by the Deputy Secretary of Interior, meet biannually to address policy issues of common interest in the DoD, intelligence, and civil communities.

The CAC provides a means for communication between the civil users of IC capabilities and the providers. Capabilities of the intelligence community, new technology developments and novel applications of data and sensors are shared. The staff of the CAC coordinates training for the civil community to better understand how to use and protect this information. Under the CAC's leadership, working groups on Global Fiducials, Thermal Event Sensing, Imagery Derived Product, Emergency Response, Security, and Requirements have been established. These groups have fostered innovative solutions to unique civil problems and provide a base of scientific experts to help solve other challenging problems.

Over the years, membership has changed and eroded. The Department of State and the Department of Energy have left the organization as voting members and now access the IC's capabilities as members of the Intelligence Community. With the creation of the Department of Homeland Security in 2002, FEMA, the U.S. Coast Guard and parts of HHS and DOT are now under the umbrella of DHS. They are currently still members of the CAC, but because DHS is part of the IC also, they have direct access to intelligence capabilities. In 2003, after the Columbia disaster, NASA signed an MOA with the National Geospatial-Intelligence Agency for direct support of its manned space flights. Although NASA is still a member of the CAC, it has not used their services since signing the MOA with NGA.

If the CAC structure is to support the additional responsibilities of homeland security and law enforcement, it will need major augmentation of resources, people, budget authority and a new charter to capture the new environment in which it would operate. It would also need new management authorities to have influence over IC and domestic user's exploitation capabilities to effectively be able to respond in time dominant situations.

Even in this changing environment, it should be noted that the CAC has served the civil community very well for 30 years. It provides otherwise unavailable data to member agencies and performs a vital role in educating civil agencies about the potential applications of data derived through intelligence systems. It is worth noting that the technical and training support provided through the CAC adds significant value to the civil agencies' use of these data. The ISG believes that any new process should build on the positive aspects of the CAC. The working group activities which foster cross-fertilization, the skilled secretariat as well as the training and education function performed by the CAC are a necessary component of any future process to support civil, homeland security and law enforcement domains.

Finding #3:

- ***Potential Law Enforcement users, and to a lesser extent, Homeland Security users do not understand how intelligence capabilities might be applied to further their missions and functions.***

Recommendations:

- ***The ISG recommends that a Domestic Application of National Capabilities (DANCAP) Program be established to facilitate a "process of discovery" for domestic users to enhance their missions and functions.***

Discussion:

The ISG believes that the creation of a Domestic Applications of National Capabilities Program (DANCAP), modeled after the "TENCAP" program, for the domestic community is vital to help insinuate domestic applications in the domains and ensure future evolution and development of systems and procedures and techniques. The purpose of DANCAP is to foster new and innovative ideas for the use of IC capabilities in solving civil, homeland security and law enforcement domain problems. This program would be initially funded by the DNI and executed by the DHS/DAO. Over a period of 10 years the program dollars would be reduced at the DNI level and increased at the execution/Agency level and sustained at the Agency level thereafter. An agency in each domain would be appointed as the focal point for the program. The ISG recommends that DHS be the lead for the homeland security domain, the FBI be the lead for the law enforcement domain and that DOI be the lead for the civil domain.

The DAO would be responsible for the administration of DANCAP. Each year it would solicit candidate projects from the three domain focal points and select the winners. The domain focal points would be responsible for soliciting ideas from their domain, prioritizing them and monitoring the funding of successful ideas in their domain. They would also be responsible for moving successful prototypes to an operational status.

Finding #4:

- ***Implications for R&D, acquisition, and Tasking, Collection, Processing, Exploitation and Dissemination (TCPED) resulting from expanded IC support to civil, LE and HLS domains must be addressed in any solution.***

***Recommendations*:**

a. DNI should place a higher priority on the needs of domestic users in the allocation of resources in existing and future TCPED architectures.

b. System requirements development process should provide a "seat at the table" for domestic users to influence R&D, acquisition of new systems and policy.

***Discussion*:**

The Civil Applications Committee (CAC) has been functioning effectively for over 30 years. It is housed in and sustained by US Geological Survey (USGS) within the Department of Interior (DOI). They host the Committee and they devote approximately 10 people to manage the infrastructure and administer the community of users meetings, educational forums, and technical exchanges necessary to gather and represent requirements. When information is collected in response to the CAC's requirements, the Intelligence Community (IC) has not always had the necessary processing and exploitation tools, techniques, and personnel to meet the needs of the civil community. To assure results are achieved that meet civil user's needs, the USGS has invested in development of its own extensive classified information technology and communications infrastructure to allow them to ingest and exploit the collected information. This model has required significant commitment and persistent support over many years by DOI and this experience serves as a useful reference in planning for a much-expanded set of customers.

With the post-9/11 creation of the Department of Homeland Security (DHS) and the national attention given to the mission of protecting the homeland, the nation's intelligence agencies have become proactive in reaching out to this agency to establish effective working relationships. Both the National Geospatial-Intelligence Agency (NGA) and the National Security Agency (NSA) have established liaison positions at DHS and each is representing DHS requirements back through the resources of their agencies while working to understand and respond to identified needs. They are also "pushing" information to DHS that may be useful as they explore their growing relationship and discover new ways to cooperate. CIA is similarly playing a significant supporting role with the provision of senior officers with analytic backgrounds to aid in the process of exploiting and using intelligence information to help DHS.

In contrast, the "law enforcement" community has virtually no significant engagement with the IC for the use of NTM collection resources. They are viewed by the IC as a major risk to "sources and methods" during the discovery process inherent in prosecutions and trials. They are also constrained by extremely limited budgets, and they generally focus on criminal activity post event rather than preventing an event. These attributes make them unappealing to the IC as a customer and partner. In cases where important and useful IC information is provided, the highly classified nature of the sources and methods involved are either placed in jeopardy in the discovery process leading up to prosecution, or the prosecution is jeopardized by potential IC decisions to not allow their information to be so used. This conflict of interests and objectives is a classic prescription for dysfunction, and has led the IC and LE communities to generally treat each other with extreme caution.

NTM systems are sophisticated and highly technical collection platforms controlled by an extensive ground infrastructure to allocate and focus collection and to process and deliver useful products in a form amenable to exploitation. The process of effectively using these systems is frequently referred to TCPED, which stands for Tasking, Collection, Processing, Exploitation, and Dissemination. To use the collectors effectively there are mature processes to "task" the resource to collect specifically identified information from some location on the globe. In this process, alternative uses of the resource are considered in light of established "priorities" and the resource is allocated to deliver the greatest return by collecting and processing the highest priority objective. The same is true for the PED portions of the process, and processing, exploitation, and dissemination resources are similarly prioritized against community-vetted requirements. This prioritization and the consequent allocation of resources must be adapted to encompass the new domestic security missions, i.e., civil, homeland security, and law enforcement. Absent adjustment, foreign intelligence and support to established IC and DOD priorities will almost always overwhelm domestic security requirements.

Beyond expanding the TCPED process to enable and encourage the inclusion of domestic security requirements, complex legal and policy questions must be addressed to support the law enforcement roles of all three domestic security user communities. In particular, changes are essential to prevent the compromise of sensitive sources and methods. Information derived from NTM must be protected while simultaneously freeing it to contribute to preventative law enforcement activities and criminal arrests and prosecutions without risking its compromise. Under current conditions, defense attorneys press for access to national security sources and methods as a means to pressure the government into abandoning prosecution. New policies and approaches to litigation are needed to harmonize these competing interests to enable the use of NTM in the civil, homeland security, and law enforcement communities.

Beyond allowing existing NTM processes to work on behalf of the domestic security community, there must be a concurrent investment in developing the techniques, knowledge, and in military parlance "doctrine" to achieve proficiency. This will require education, experimentation, discovery, and development of techniques and systems tailored to this new mission. It will take sustained funding to perform research and development and to conduct experiments that explore new uses and applications. This investment is comparable to that made by the military under the TENCAP program which stood for Tactical Exploitation of National Capabilities. This program was first established by the Army in 1973 and it was expanded to all the services at the direction of Congress in 1977. It was a highly successful effort that helped the NTM systems become fully integrated into military training, exercising, operations, and planning. A similar investment will be essential to achieve comparable integration of NTM capabilities in the mission and doctrine of domestic security users.

Finding #5:

- ***Current policies governing use of intelligence capabilities to support domestic users have not been updated to reflect Post 9/11 priorities, new legislation and threats to the Nation. These policies and inconsistent interpretation of these policies continue to promote use of national assets only as a last resort with a highly risk averse approach to approval.***

***Recommendations*:**

a. DNI promptly convene a policy review, including the legal basis for policy, across all agencies with the eye towards promoting a more efficient and effective use of intelligence capabilities for domestic support.

b. Specific attention needs to be provided to any executive orders that in the view of the DNI prevent needed change and if appropriate seek changes in those executive orders.

c. If necessary, amend E.O.12333 to provide clear guidance on the role of the IC in support of domestic users.
- ***Provide Executive guidance to encourage effective use of intelligence capabilities for civil, homeland security and law enforcement purposes and enable flow-down of this guidance through departmental directives.***

d. DNI, in coordination with the DOJ, DOD and DHS, establish a fast-track process for authoritative legal guidance and policy review.

e. DNI should publish policy governing access and use of domestic IMINT and MASINT.

f. DNI should delegate approval authority for domestic user imagery tasking, collection, processing, exploitation and dissemination to the D/NGA.

***Discussion*:**

"We agree on essentially all areas...except for those where we disagree."
- lawyer

During the course of the study, and in particular as a result of presentations by lawyers from the intelligence community, the ISG was advised of the uncertainty and conflicting opinions regarding lawful application and use of imagery, imagery intelligence (IMINT) and measures and signatures intelligence (MASINT) for domestic purposes. This conflict and resulting uncertainty also surfaced in the development and application of relevant policy.[3]

[3] Procedures for collecting domestic SIGINT are well established and governed by Attorney General Guidelines, minimization rules, and procedures implementing the Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. 1801, et seq.

For example, although the courts have permitted warrantless aerial searches of private property, there are no cases involving the use of satellite technology.[4] Consequently, legal opinions are based on interpretations of cases similar in subject matter and policy is written relying on these opinions. The ISG has observed the result of this approach is that the legal and policy communities have adopted a risk averse rather than a risk management philosophy. This is especially evident when the IC is considering whether to proceed in matters not clearly governed by settled case law.

A further complication is rapidly changing technology in both public and private sectors. Its profound impact on data collection is not met with concomitant changes in policies to accommodate new technology. The U.S. Supreme Court's 2001 decision in *Kyllo v. United States*, [5] holding the use of a hand-held thermal imaging device to scan a private residence to determine if the amount of heat emanating from it was consistent with high intensity lamps typically used for indoor marijuana growth constituted an unlawful warrantless search has caused much debate and uncertainty within the IC legal community. Although this decision has placed in question the continued viability of past settled practice of the IC within the domestic domain, to date we are not aware of any clear authoritative guidance issued on the impact, if any, of this decision. Further, *Kyllo* may impact the use of domestic MASINT as well. There is little if any policy guidance or procedures regarding the collection, exploitation and dissemination of domestic MASINT.

The cumulative affect of the risk-averse approach now taken in the IC to address difficult and complex legal and policy issues causes delay, uncertainty and may result in missed opportunities to collect, exploit and disseminate information critical to the anti-terrorism, homeland security and law enforcement missions.

In the mid 1970's, Congress examined allegations that classified imaging collecting systems were being used to illegally spy on U.S. citizens. To address these allegations, President Ford established the Rockefeller Commission to review the entire range of classified overhead photographic sensor capabilities that were being used for imaging domestic areas. The Commission did not substantiate the allegations of illegal uses of these capabilities, rather, it concluded the use of these systems by Federal civil agencies was appropriate and desirable uses of costly nationally funded classified resources. However, the Commission did point out there was a lack of oversight authority for these activities. The President responded by directing the formation of a Civil Applications Committee (CAC) to allay concerns about improper or illegal uses of such systems.

The ISG believes that as more IC capabilities are used to support domestic civil, homeland security and law enforcement missions the same concerns which gave rise to the CAC are likely

[4] California v. Ciraolo, 476 U.S. 207 (1986) (No warrant required for an aerial search of an enclosed yard adjacent to a residence.); Dow Chem. Co. v. United States ex rel. Administrator, EPA, 476 U.S. 227 (1986) (Use of a highly sophisticated mapping camera to photograph the interior of an industrial facility did not require a warrant.); Florida v. Riley, 488 U.S. 445 (1986) (Court upheld a low altitude search by helicopter of a greenhouse missing roof panels.)

[5] 533 U.S. 27 (2001)

to emerge again. Although the tragic events of 9/11 and continued efforts to fight the global war on terror have created an environment quite different from that of the mid-1970's, the ISG believes appropriate safeguards to ensure the capabilities of the IC are used lawfully and with full consideration of the rights of U.S. persons are needed. In response to many factors, including the Report of the 9/11 Commission, Congress passed the Intelligence Reform and Terrorism Prevention Act of 2004, (IRTPA).[6] The IRTPA establishes the Privacy and Civil Liberties Oversight Board in addition to charging each agency to establish a civil liberties office. The ISG believes this Board may provide an appropriate means to assure the US public that IC capabilities are being used lawfully and in a manner sensitive to the civil and privacy rights of US persons.

In addition to the IRTPA, Congress responded to 9/11 by passing The Homeland Security Act of 2002,[7] and the USA PATRIOT ACT.[8] The ISG noted that many administrative authorities such as directives and policies of the federal government, and in particular the IC, have not been revised or amended since 9/11. While the ISG did not attempt a comprehensive review and cataloging of all such documents, some fundamental policies need to be addressed.

The first is Executive Order 12333, United States Intelligence Activities, (1981). During the study, it became clear to the ISG that despite a reluctance on the part of the IC to review this executive order with a view to amend it, such a review is necessary.[9] The ISG heard any number of instances in which domestic requirements for IC resources were either very difficult to satisfy, or justifications were strained in order to meet policy requirements. For example, geospatial information obtained from imagery taken over the United States should be recognized as a class of information, which, by its very nature should seldom be subjected to a rigorous pre-collection, exploitation and dissemination process, as other data sets or requests for collection rightly should be. E.O. 12333 should be amended to permit as unfettered an operational environment for the collection, exploitation and dissemination as is reasonably possible. It is time to clearly articulate national policy and rules for employing IC capabilities in a robust manner to meet domestic civil user's needs.

Additionally, the ISG noted the decisional authority for the use of domestic imagery does not rest with the IC functional manager for imagery, the Director of the National Geospatial-Intelligence Agency. The Director of Central Intelligence Directive setting the policy for imagery should be reviewed and amended to align authority with responsibility.[10]

The cumulative impact of the presentations to the ISG made clear there is an urgent need for a top-down, Executive Branch review of all laws and policies affecting use of intelligence capabilities for domestic purposes. The product of this review should be a legal and policy

[6] "Intelligence Reform and Terrorism Prevention Act of 2004," Pub. L. 108-458, Dec. 17, 2004.
[7] Pub. L. 107-296, Nov. 25, 2002.
[8] "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001," Pub. L. 107-56, Oct. 26, 2001.
[9] Amended by: E.O. 13284, Jan. 23, 2003(Adding certain elements of the Dept. Of Homeland Security to the list of members of the intelligence community); E.O. 13355,Strengthened Management of the Intelligence Community, Aug. 27, 2004.
[10] Director of Central Intelligence Directive (DCID) 1/8, March 21, 2001.

framework that promotes a more efficient and effective use of intelligence capabilities but tempered and guided by appropriate concern for the privacy and civil liberties of US persons.[11]

Finding # 6:

- ***The timely and efficient provision of geospatial intelligence support to domestic users is impeded by policy barriers, classification issues and culture.***

***Recommendations*:**

a. ***Set threshold resolution of Imagery Derived Products at 0.5 meters.***

b. DNI develop the ability to provide NTM imagery at 0.5 meter resolution without the burden of classified handling to the domestic users community.

***Discussion*: (See classified Appendix VIII for a detailed analysis)**

A recurring theme in ISG interviews with stakeholder agencies and organizations interested in civil, homeland security, and law enforcement applications centered on timely and efficient access to classified imagery data. Three key factors are perceived to influence the timely and efficient provision of classified imagery and advance geospatial intelligence (AGI) data to customers in the Homeland Security, Civil, and Law Enforcement domains:

- A cultural aversion toward collection of domestic imagery based on concerns involving the potential for congressional oversight sanctions centering around 4th Amendment rights.
- Policies that pose hurdles to the timely and efficient dissemination and exploitation of classified data from national sources.
- Security constraints posed by data classification.

These factors are curiously intertwined in a complex and dynamic operating environment where the imagery community deals with domestic imagery collection and dissemination of the resulting data and products as an exception to policy. That environment may prove to be a formidable hurdle in trying to support homeland defense, civil, and law enforcement activities that are largely domestic in nature.

[11] An approach would be to actively use the Privacy and Civil Liberties Oversight Board, established in section 1061 of the, "Intelligence Reform and Terrorism Prevention Act of 2004," Pub. L. 108-458, Dec. 17, 2004, for the oversight of the domestic use of IC capabilities.

CULTURE

The domestic imagery environment has its roots in the mid-1970s amidst a power struggle between the legislative and executive branches over US intelligence activities. Two events during this period had direct and lasting impact on the imagery community:

- In 1975, the Civil Applications Committee (CAC) was chartered to oversee appropriate and desirable uses of classified imagery by Federal civil agencies.
- President Ford issued E.O. 11905 in February 1976, dealing with concerns on domestic spying and establishing the parameters within which US intelligence organizations could operate. E.O. 11905 was superceded by E.O. 12333, which remains in effect.

The imagery community practices a self-policing approach toward domestic collection requiring detailed documentation and a legal review of requests for tasking national imagery assets. Any agency or organization requiring domestic imagery collection[12] from classified national systems or from commercial sources acquired by the National Geospatial-Intelligence Agency (NGA) submits an annual Proper Use Memorandum (PUM) that defines their requirements, intended use, and an acknowledgement of awareness of the legal and policy restrictions regarding use of domestic imagery. A high-level legal review is conducted to ensure that appropriate measures are being followed when collection activity is undertaken. This collection by exception to policy approach is hardly supportive of the homeland security, civil, and law enforcement communities where the greatest emphasis is on domestic collection.

POLICY

Policy governing use of classified satellite imagery reconnaissance data is anchored in a complex web of law, National Security Policy and Presidential executive orders, DNI/DCI and DOD Directives, Interagency Agreements, and imagery-specific policy developed, coordinated, promulgated and maintained by the National Geospatial-Intelligence Agency implementing these higher authorities.

The IC manages and adjusts policy associated with the imagery release and disclosure process supporting non-IC access to classified imagery and imagery data, weighing national security interests against the need for greater openness. Within the last decade, policy strides have been made in making imagery and imagery-derived data accessible at the level of classification appropriate for the specific user. Data can be disseminated at the UNCLASSIFIED level in support of demonstrated needs for users that do not normally have access to classified materials. The fundamental policy approach to broader imagery sharing across the homeland security, civil, and law enforcement domains seeks to answer the question:

[12] Domestic imagery is defined as imagery collected from classified national reconnaissance platforms covering the land areas of the 50 United States, the District of Columbia, and the territories and possessions of the United States to a 12-nautical-mile seaward limit of the land areas. U.S. Federally owned or Federally operated property, including military bases, U.S. military ships in foreign ports, or U.S. embassies in foreign countries may be imaged as a non-domestic target. However, a target objective of a specific U.S. person at these sites is generally not appropriate.

What degree of protection is necessary and appropriate in a complex, dynamic operating environment with demands for wider dissemination of imagery and imagery-derived resources?

Organizations with missions and responsibilities that have traditionally required access to imagery and products from classified systems may be well-grounded and even participate in developing the policies supporting acquisition, exploitation, and dissemination of classified national satellite imagery data. Federal civil agencies and organizations that have CAC representation have had a means for embracing national policy since 1975. Establishing familiarity with the policy chain for non-CAC civil agencies, and non-federal consumers will be a challenge if the IC is to broaden access to national assets.

CLASSIFICATION

Security constraints based on classification can impede the use of national imagery data by non-IC personnel. At many locations in the homeland security, civil, and legal domains, the problem is magnified when customer organizations have no security mechanism to facilitate access to and exploitation of classified imagery assets. Protection of sensitive intelligence sources and methods is the fundamental reason underlying classification of national satellite imagery and products derived from that data. This "armor of security" has been maintained for more than four decades because the investment in satellite reconnaissance has been high, the benefits enormous, and the Intelligence Community remains convinced that wide dissemination of the intelligence product increases the probability of a compromise that could result in neutralizing the investment.

It is rare that any single factor renders an image, set of images, or data derived from that imagery classified. The IC has established a classification regime that seeks to maximize data availability without exposing national satellite imagery reconnaissance capabilities to an extent that would facilitate the development of incurable countermeasures. In practice, however, the classification of national imagery and imagery products is generally an across-the-board application of a SECRET level marking in an effort to protect sources and methods and serve as a hedge against uncertainty. That approach is captured in Executive Order 12951, which mandates that all imagery except from systems declassified by Presidential order in 1995 shall be kept Secret in the interests of national defense and foreign policy.[13]

The perceived necessity to safeguard sources and methods precludes declassification of most PIR source material.[14] Decisions to declassify and release data are predicated on a number of security concerns. For example, if a release of classified imagery reveals information on the strategies and sensitive capabilities used for effective collection, an adversary could use that information to negate the collection capability. Denial or limitation of access to previously accessible observations used to support U.S. policymakers can have serious consequences, including the possible compromise of U.S. military actions.

[13] Executive Order 12951, Release of Imagery Acquired by Space-Based National Intelligence Reconnaissance Systems, Section 2(a), 22 February 1995.

[14] Primary Image Record - the primary imagery collection product, including the original digital data record, original negatives, duplicate positives, and/or duplicate negatives with associated titling and marginal data.

As technology and policy expand the boundaries of what types of imagery and imagery products are accessible by the public, the guidelines for classifying imagery on the basis of source alone should shift in a corresponding way. Decisions on retaining classification simply on the basis of resolution will no longer be valid; impacts from other criteria, e.g. the metric accuracy of a particular imaging sensor must be used. The rationale for maintaining a stricter classification regime for imagery and products from current national programs may well be challenged by future commercial endeavors.

In an environment, where 0.5-meter resolution panchromatic electro-optical satellite imagery is commercially available, classification decisions should be predicated on protecting capabilities that are *unique* to the USG assets. Arguments that the availability of high-resolution commercial imagery justifies declassification of some classes of national systems data, particularly the electro-optical data, face the counter argument that the availability of high resolution commercial imagery provides a data source that should be exploited instead of considering declassification of the national source, removing the requirement to jeopardize other unique capabilities.
Perhaps the most perplexing and insurmountable issue surrounding the declassification of satellite imagery centers on the implications of Freedom and Information Act (FOIA) requests from the public. If the IC released information and imagery derived directly from classified systems, could it still protect technology, imagery, and intelligence reports from compelled release pursuant to the FOIA.

In addressing the issues associated with access to classified imagery information at all levels (including State, local, and tribal governments where security clearances for national data are rare), the IC will have to consider whether to work largely in the current environment, or move to a large-scale declassification regime requiring new legislation or high-level policy to ensure the Director of National Intelligence (DNI) will have the tools and authority to protect the remaining sensitive reconnaissance sources. Concurrently, the imagery community will be required to address resource implications for conducting classification reviews and responding to an increasing number of Freedom of Information Act requests. Finally, the real key to success is to make the classification system understandable and emphasize better education on the needs for proper security.

Finding #7:

- ***Effective IC support to federal, state, tribal, local and private sector authorities is complicated by overlapping jurisdictions and barriers to information sharing.***

***Recommendations*:**

a. DHS information sharing authorities be exploited to their fullest.

b. The IC must provide information and data in a form that permits sharing with state, tribal and local law enforcement entities, i.e., "write for release."

***Discussion*:**

The ISG concluded that there are many organizations with overlapping responsibilities in the Homeland Security and Law Enforcement domains. These overlaps exist both within the domains as well as between the domains. Certainly the ISG recognizes that some overlap may be necessary due to the unique responsibilities of an organization. It could also be posited that we need many organizations looking at these complex domains because it provides a richer and more thorough assessment from a multitude of perspectives. That could be true if information sharing were a fundamental requirement for all of the organizations. What in fact seems to happen is that each organization claims "ownership" of the information. Many of the organizations that briefed the ISG reported that "ownership" of info was a significant impediment to the sharing of info. The 3rd party rule, ORCON and LIMDIS are but three examples of ownership that impedes the sharing of information by requiring specific approval from the originating organization before further release is permitted. Another consequence of this situation of overlapping responsibilities is that it is difficult to determine who is in charge--- or, everyone thinks they are in charge. This overlap complicates the effective access to technical IC capabilities.

Border protection is an example where several federal organizations have overlapping responsibilities. DHS has the responsibility to secure the majority of our borders and exercises those responsibilities through the Customs and Border Patrol (CBP). But that responsibility does not extend to areas where the Bureau of Land Management (BLM) or the Department of Interior (US Forest Service) "owns" the land on the border. To fulfill their responsibilities, each of these organizations has its own law enforcement element, and its own intelligence/ information requirements. Access to technical IC capabilities by these organizations to meet these intelligence/information requirements is very limited, if at all, and not coordinated. CBP could access these technical IC capabilities through DHS. DOI and BLM are members of the CAC, but have limited or no access to technical IC capabilities for homeland security (HLS)/law enforcement (LE) needs. Therefore, the application of technical IC capabilities to border protection for this Nation is very complicated and extremely limited, in part due to overlapping responsibilities.

Overlapping roles within the law enforcement domain complicate the effective use of technical IC capabilities. The FBI is the Nation's lead federal law enforcement organization. However, the DHS is a unique organization with both HLS and LE responsibilities embedded in its elements, such as CBP, ICE, Secret Service, USCG--- which in some cases overlaps FBI LE responsibilities. NOAA, BLM, DOI, EPA and others also have organic law enforcement responsibilities and capabilities. Each organization has its own process for accessing technical IC capabilities, if they choose to do that, which in many cases they do not. And when they do, it is frequently done in a reactionary context rather than as a proactive application. In many cases, the organization will go directly to the provider, such as NGA. In other cases, they may go to the CAC. There is no single source for the LE requirements---they may come from a multitude of players. Nor is there a single process to access the capabilities provider as the CAC is not

charter to support the law enforcement domain. All of this leads to ineffective access to technical IC capabilities.

Federal support to state and local governments is another example of where considerable overlap exists. The FBI using the JTTFs, DHS using the Homeland Security Operations Center and the Homeland Security Information Network (HSIN), the US Marshals Service through its Technical Operations Group (TOG), the National Guard through each states' Adjutant General, NGA and NSA and others have all developed processes for providing support to state and local governments. This is certainly a critical and commendable effort. However, due to the overlap that is created by the multitude of means available, state and local governments do not have effective access to technical IC capabilities.

The Department of Homeland Security has broad information sharing authorities. Sections 201 and 202 of The Homeland Security Act requires that all Homeland Security information will be given to DHS, and will be disseminated by DHS. An Information Sharing MOU dated March 4, 2003 is a sweeping interagency agreement which is binding on DHS, Intelligence Community, DOD, Treasury and *all* Federal LE agencies and specifically defines the types of information that are required to be reported from those organizations. HSPD 7 provides the authority to the Secretary of DHS to look government-wide to satisfy GEO-INT HLS requirements.

Finding #8:

- ***The exploitation, fusion, storage and sharing of "domestic information" is complicated because current rules require extensive special handling protections.***

***Recommendations*:**

a. DNI in conjunction with the Attorney General promulgate guidelines to promote as appropriate the effective exploitation, fusion, storage and sharing of domestic information.

b. Assess the need for legislative solutions to ensure a rational policy framework is implemented to meet the requirements of a post 9/11 environment.

c. Issue a DNI Directive for the emergency disclosure of classified intelligence information consistent with the provisions of E.O. 12958.

***Discussion*:**

Once information is developed from national technical means (or from any national intelligence or information gathering function), the presence, content, meaning and handling of that information are of professional concern. The reasons for this are painfully obvious to even the casual observer. Protection of the sensor, source and method is a critical requirement. Indeed,

protection of the technology and the methodology used to develop certain technical detail is sometimes so sensitive that the information itself must be highly classified in order to protect the capability.

However, in the domestic context, there is another level of concern requiring technical, procedural and legal monitoring. It is possible to violate, even in the best of conditions and with the best of intent, the constitutional and legal rights of our citizens. In the fight against terrorism and against crime with national (homeland) security implications, in the domestic context, it is imperative that we address not merely the technical facts surrounding such collection but also their broader and deeper meaning in the context of our citizenry and their right to privacy and freedom from excessive governmental intrusion into their lives. In short, we need to engage in these activities under the rule of law.

Things have changed since the act of terrorism on 11 September 2001 that created broad destruction and generated mass casualties here in the United States. Suffice to say that the rights of free access and open transportation (and other elements of our pre-9-11 society) enjoyed before those pivotal events have now been abridged at least in practice if not in law. We have come to refer to this change in its totality as the "new normal" since we have achieved over time a national homeland security condition less restrictive than that which resulted immediately after the attack but still far different – more restrictive and more controlling -- from that which existed before the attack. In some cases this "new normal" condition is passive and defensive, albeit expectant of another attempt or another attack. In other cases the "new normal" is active and offensive and seeks to preclude or to interdict another attack. We see it as a government imperative to clarify the legal, policy and procedural context in which the "new normal" can be effectively achieved without violating generally accepted societal and cultural norms. The question is very simple: How do we protect our citizenry while preserving our culture and guaranteeing their constitutional rights? The answer, seemingly, is very complex.

Every part of the intelligence information system applied to the problems posed by terrorism, crime with national (homeland) security implications, and even disasters and other forms of instability, is affected by this circumstance. Thus in ISG deliberations great care was taken to include legal, policy and procedural ideas in our discussion and much effort was made to inquire into the legal conditions under which domestic information gathering and intelligence activities related to national technical means are undertaken.

Our findings indicate that the collection, exploitation, integration, storage, sharing and application of information in the domestic context is complicated for all the reasons noted above and will require special handling and specific policy and legal protections.

Another feature of the challenges we face is the inclusion of law enforcement support – currently generally excluded under the CAC portfolio as it is now put into practice. Should the law enforcement community, including the federal, state, local, tribal and private sector, be supported by NTM through the CAC? There is no easy answer, but consider the possibility that information derived from NTM could be critical in empowering law enforcement action to interdict or preclude a terrorist activity from occurring. Could we legitimately say – especially in the weapons with mass effects context – that information that might have been acquirable or even

available could not be provided to law enforcement because our legal and procedural structure did not provide for it?

The ISG believes strongly that the legalities and procedural mechanisms needed to facilitate, limit and otherwise control the gathering and application of information and intelligence by national technical means, should be rapidly developed and promulgated throughout the policy and operational elements of the various parts of the homeland security, law enforcement and civil communities. It seems paramount to establish the boundaries and methodology, in their legal context, before we do anything else. Without that supporting structure upon which to base our actions we have little to guide us and less to substantiate our views and beliefs (or to change our views and beliefs).

In some cases we have – in the present context of the Department of Homeland Security and in the activities of the Federal Bureau of Investigation – already begun to deal with the handling of domestic information similar in sensitivity and meaning to that gathered through NTM. There is a growing body of legal decision and Congressional action that seems to provide the potential for relevant interpretation and applicable case law. There are a host of Presidential memoranda and executive branch decisions that direct certain actions and events that are germane. But even in the face of all these possibilities we still cannot say what the law allows or does not allow with certainty. The problem as the ISG sees it is that nowhere can we find an interpretation and firm contextual description of the substance of this new post-9-11 condition.

Finding #9:

- ***Civil agency archival holdings are extensive, but uncoordinated. They may represent an important source of data for research and potential new applications within the civil, law enforcement and homeland security domains.***

***Recommendations*:**

a. DOI create a master list of remote sensing holdings

b. DHS spearhead a multi-disciplinary effort to understand the holdings, identify uses, and develop methods to demonstrate utility of the holdings

c. DNI, DOD, and civil agencies should collaborate to better optimize national collection holdings for improving domestic use.

***Discussion*:**

The United States is one of the few remaining countries that segregates its space program into national security, civil, and commercial space, with thick and complex bureaucratic boundaries

between them, and creating great inefficiencies in the overall national remote sensing program. The homeland security mission offers one opportunity to improve upon that.

The ISG heard testimony about the extensive remote sensing holdings within the U.S. civil and scientific community. Remote sensing data is not only collected by government organizations like NOAA and NASA, by also by the U.S. Geological Survey and the Department of Agriculture. In fact, the CAC model, as described to the ISG, has always operated on a "not to interfere" basis with U.S. intelligence requirements, in part because of the availability of substitute or complementary data to support civil agency missions.

Fulfillment of the data and exploitation needs of the domestic information requirement have the potential, over time, of being an extensive resource drain on the national intelligence system, with some implication for the foreign intelligence mission. (The ISG does not see such an extensive resource competition at this time, however). First consideration of the extensive civil holdings may limit the amount of resources required from the more costly intelligence system. Of course, the ultimate value proposition may relate much more to timeliness of access, ability to exploit, precise nature of the source, or other criteria.

Of concern to the ISG is the fact that very little of this civil agency data – gathered under substantially different legal authorities and with few sources and methods sensitivities – appears to be used, even experimentally within the law enforcement and homeland security communities, in particular. While also resource constrained, the U.S. civil and scientific community represents a potentially important source of knowledge and data from which to stimulate experimentation in the use of remote sensing data for domestic applications. Moreover, collaboration between the civil agencies and the law enforcement and homeland security communities appears to be potentially less sensitive than a similar relationship with intelligence.

As the nation searches for methods to improve information and intelligence sharing for homeland security, the ISG believes that geospatial information – often, but not exclusively, maps and map products – are a compelling tool for sharing information. While localities and police services may differ in their sophistication with remote sensing data and technology, virtually everyone has familiarity with maps and map products as decision aids. This is an area where both the Intelligence Community and the civil agencies have extensive experience providing information, even information derived from sensitive sources.

Finding #10:

- ***There is a need for examining the procedures for reporting of U.S. person data including more rapid transmission of identity in specific threat situations.***

***Recommendations*:**

a. ***The ISG recommends that careful thought and design be given to a U.S. person information template that includes an assured identification of the person, an explanation of the context in which the information has been collected and processed, and the limits on distribution and use of the information.***

b. ***If allowable by statute, and not prohibited by the FISA process, a unique identification number to permit tracking of an individual should be assigned when the provision of the identity is not appropriate.***

***Discussion*:**

In our discussion with DEA, NSA, NCTC and DHS, the issue of quickly transmitting personal identification information to appropriate law enforcement organizations in a timely manner is a serious problem. Under current guidelines, when information is acquired about an illegal activity taking place in the United States that may include U.S. persons, the information is sanitized before it is disseminated to government agencies. For example, person A and person B are meeting next week at a hotel in St. Paul, Minnesota for the probable purpose of transacting a drug deal. If DEA or any other agency wants to know the specific details about who the people are, when and where the meeting is to take place so that they can take action, they must request it from the producing agency. The producing agency then retrieves the raw information and transmits it to the requestor for action. This time delay can have a serious impact on the ability to apprehend criminals in situations where time is vital to the success of a mission.

When collected information provides vital information about the commission of a crime in the U.S., the complete report should be transmitted immediately to the appropriate law enforcement organizations for action. Those agencies need to have the authority to determine if the personal data needs to be retained and how best to protect that data under current legal guidelines.

Another issue was raised with the ISG concerning effective tracking of individuals. A need was identified to assign a unique identifier to a person or organization so that their activities can be tracked over time. No need for specific person identification is seen, just a means to associate disparate activities in time and place with the same actor(s).

Finding # 11:

- ***Although the ISG has not identified the need to change any laws, it is inevitable that certain recommendations will cause concern among some segments of the body politic. A concerted effort is needed to assure a balanced discussion of the benefits and risks associated with expanded domestic use of IC capabilities.***

***Recommendation*:**

a. The DNI, senior leaders of the intelligence community and others in the Executive Branch, should look for opportunities to inform the public on the intelligence challenges associated with the war on terror.

b. Provide for the oversight of domestic uses of IC capabilities by the Privacy and Civil Liberties Oversight Board, established in the IRTPA (potential amendment to E.O.12333).

c. Domestic Applications Executive Committee should include the DNI Civil Liberties Protection Officer as an advisor.

***Discussion*:**

This section deals with the political implications of using technical IC capabilities within the US, and the critical need for the DNI, in concert with the Administration and Congressional officials, to make the case to the American people for using such technical means – including constraints and oversight – associated with doing so.

Historically, since the earliest days of the Republic, the American people have held a high suspicion of standing armies and the functions that support it, especially intelligence. Americans have always preferred the concept of intelligence as a function that supports warfighters in wartime, and as something that is done overseas, vice at home. Within this longer view, the Cold War reality of a large, prominent, and permanent U.S. intelligence community was an exception to the rule, rather than the preferred case. Both the Cold War mission and the abuses investigated by the Church and Pike Committees, and the Rockefeller Commission, reaffirmed and even strengthened this notion within the American psyche.

This uniquely American view of intelligence exists today, and may even be returning to a more historical view of a diminished intelligence community. Even given the events of 9/11 and more extensive evidence of a threat – perhaps existential – to our homeland, initiatives designed to improve intelligence have met with strong, and often uninformed public reaction. While there are perils in the comparison, one needs to look only at the response to the Patriot Act to understand the potential reaction to a broadening of Intelligence Community activities in the homeland.

Based upon the testimony given to this ISG, there are some real ironies associated with this, and some very important work to be done. First, while the Intelligence Community's reaction to domestic scrutiny in the 1970's was appropriate, and understandable, it is clear that those events created a hyper-conservative view of what can be done, as laid out in policy, regulation and practice, and one that continues today. Practices like the CAC's avoidance of law enforcement support and NSA minimization, on the one hand, reflect the serious attention that Intelligence Community leaders give to avoiding even an appearance of impropriety, yet there seems to be

little creativity for providing intelligence support except in cases where the threat appears to be compelling, such as an imminent terrorist threat.

Intelligence managers and overseers should not look for "black and white" distinctions in thinking about providing intelligence support for the homeland. A period of considerable experimentation and discovery should take place, as much within the consumer communities – law enforcement, homeland security, and the civil and scientific communities – as driven from within the Intelligence Community. Distinctions based on phenomena – SIGINT, GEOINT, and MASINT – experience of the user, and even the context of the intelligence support should be carefully considered in order to optimize support while maintaining a thoughtful perspective on the real and perceived impacts of these actions on the legitimate rights of American citizens. As is the case with the PATRIOT Act, consideration should be given to discovery periods – one, two, or three years – within which intelligence capabilities should be used experimentally, with ongoing dialogue between the IC, user, and oversight committees. All communities, but especially the user community, should be sensitized to both the potentially intrusive nature of these capabilities and the sensitivity of the sources and methods. These discovery periods should be used to inform both legal and policy regimes as they evolve, more thoughtfully and inevitably slowly.

Finally, to return to the initial theme, the public debate about the future of U.S. intelligence is well underway. While it has been catalyzed by the 9/11 Commission, the WMD Commission, and a slate of other activities, it often appears to be a debate with only one voice, often ill-informed and sometimes completely uninformed. The Administration, the Congress, and the Intelligence Community must inform this debate, credibly, on the challenges of intelligence support in the war on terror, and especially on the methods taken to protect the legitimate rights of American citizens.

CHAPTER 3: OTHER MODELS CONSIDERED

There were four other models that the ISG gave detailed consideration to but did not select. The first model was referred to as the enhanced CAC model (**Figure 8**). This model expanded the current CAC structure and process to include the homeland security and law enforcement domains. The ISG felt that a committee structure was not the most efficient process and that without multi-department level support and dedicated resources it would not be sustainable. Finally, access to a robust IT infrastructure to support a digital end-to-end environment would not be readily available.

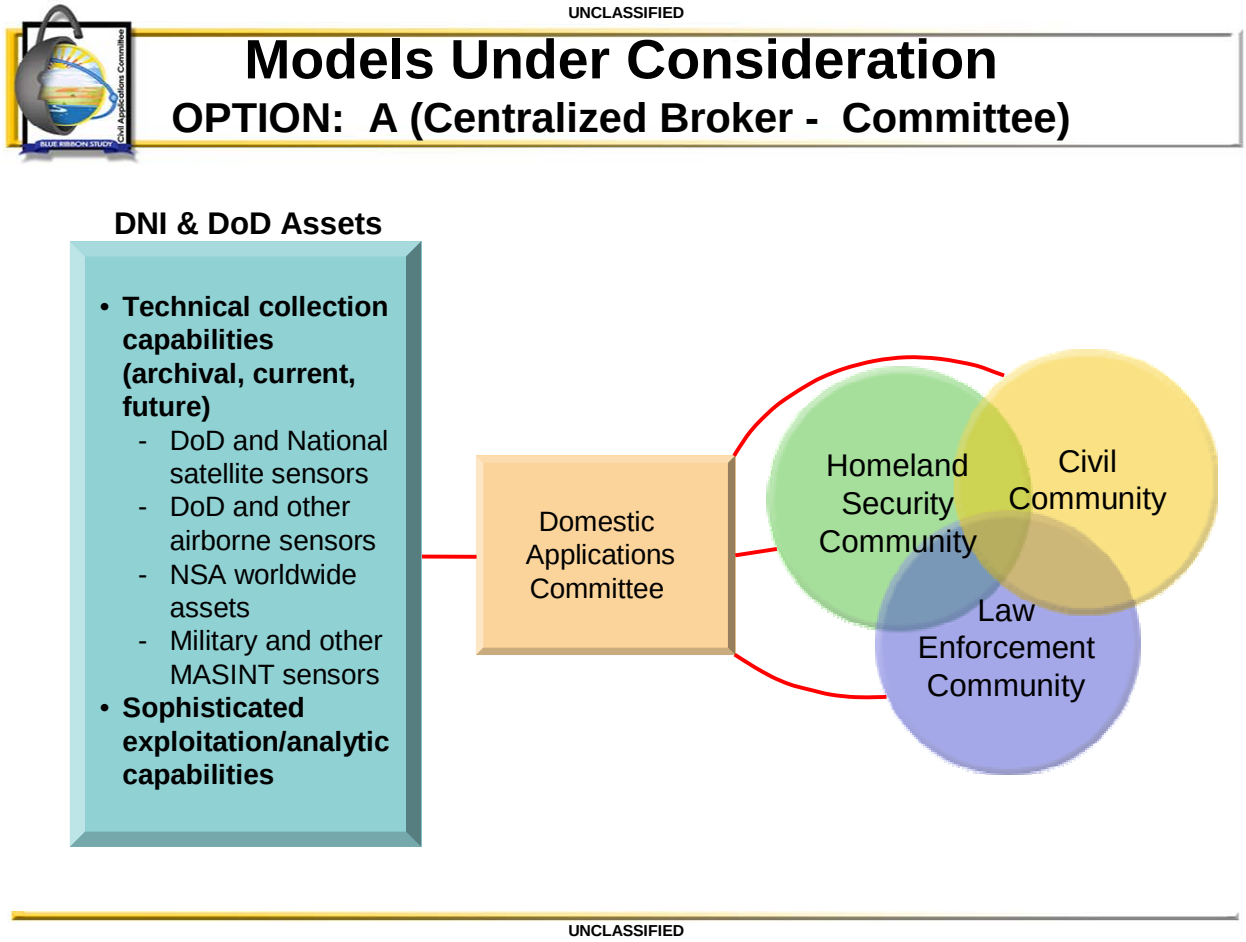

Figure 8.

The second model considered (**Figure 9**) was identical to the selected model with the exception that it was located within one of the traditional Intelligence Community agencies such as NGA. The primary factor against this model was the belief that public perception would be that the U. S. government i.e. the Intelligence Community, was spying on Americans. Therefore, avoiding even the appearance of the IC being in direct day-to-day control of the domestic information activities of the DAO is critical to a successful implementation of the new model. There was also a concern that domestic collection requirements would not compete well against foreign requirements in this model because the IC controlled the process.

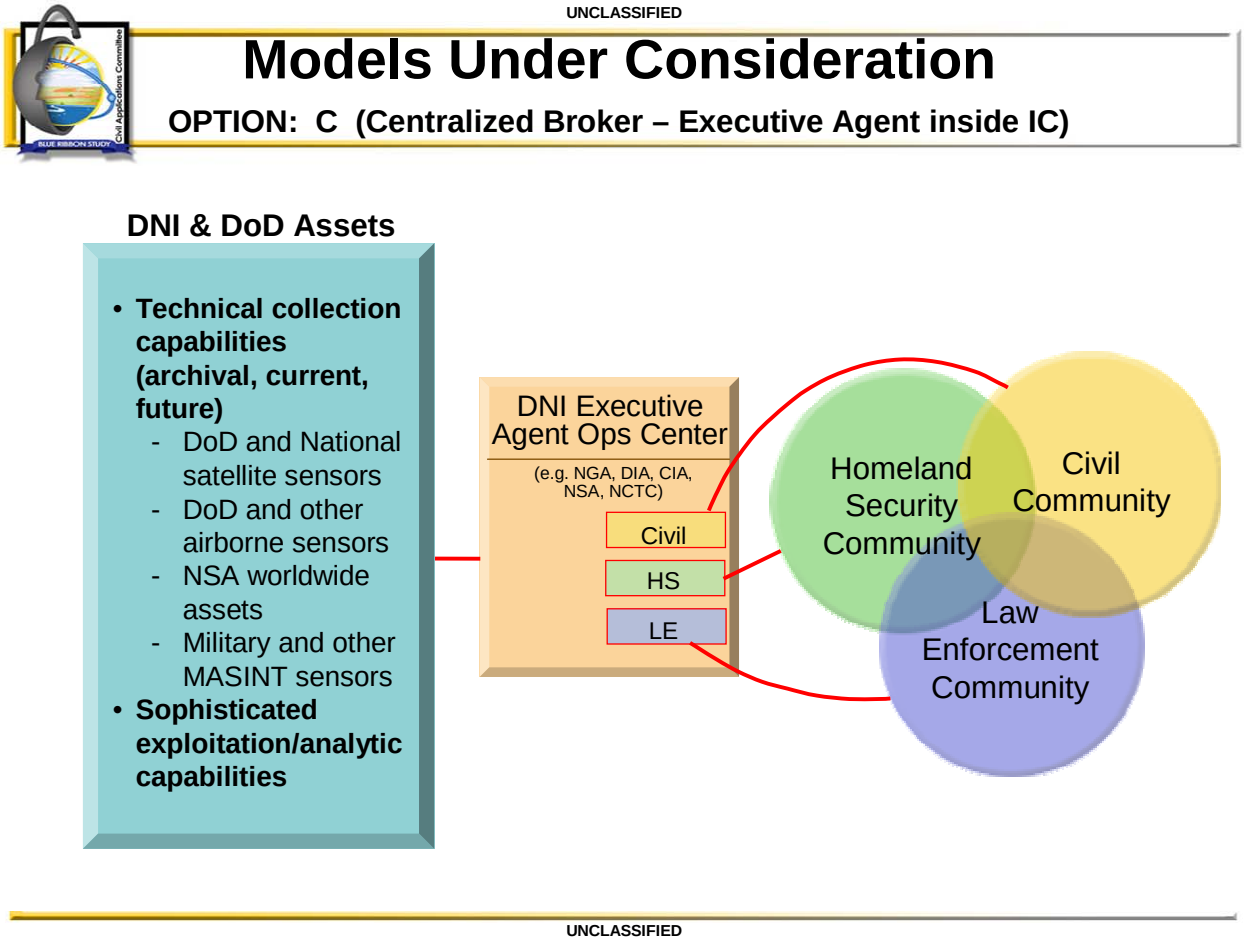

Figure 9.

The third model used a dual track to process requirements (**Figure 10**). Civil and homeland security domain requirements would be processed in DHS and all law enforcement domain requests would use the FBI as a focal point. The obvious shortcoming of this model is the duplicate centers, which unnecessarily increase the cost of the program and systemically creates an environment for more duplication throughout the process and limits sharing of information, lessons learned and lowers the chance for multi-int solutions. Because each of the three domains has law enforcement responsibilities there is no clear requirements path. In fact, the model encourages the use of whatever path will offer success. Finally, that the model may still promote a pre 9/11 view of roles and responsibilities and therefore further reduce information sharing.

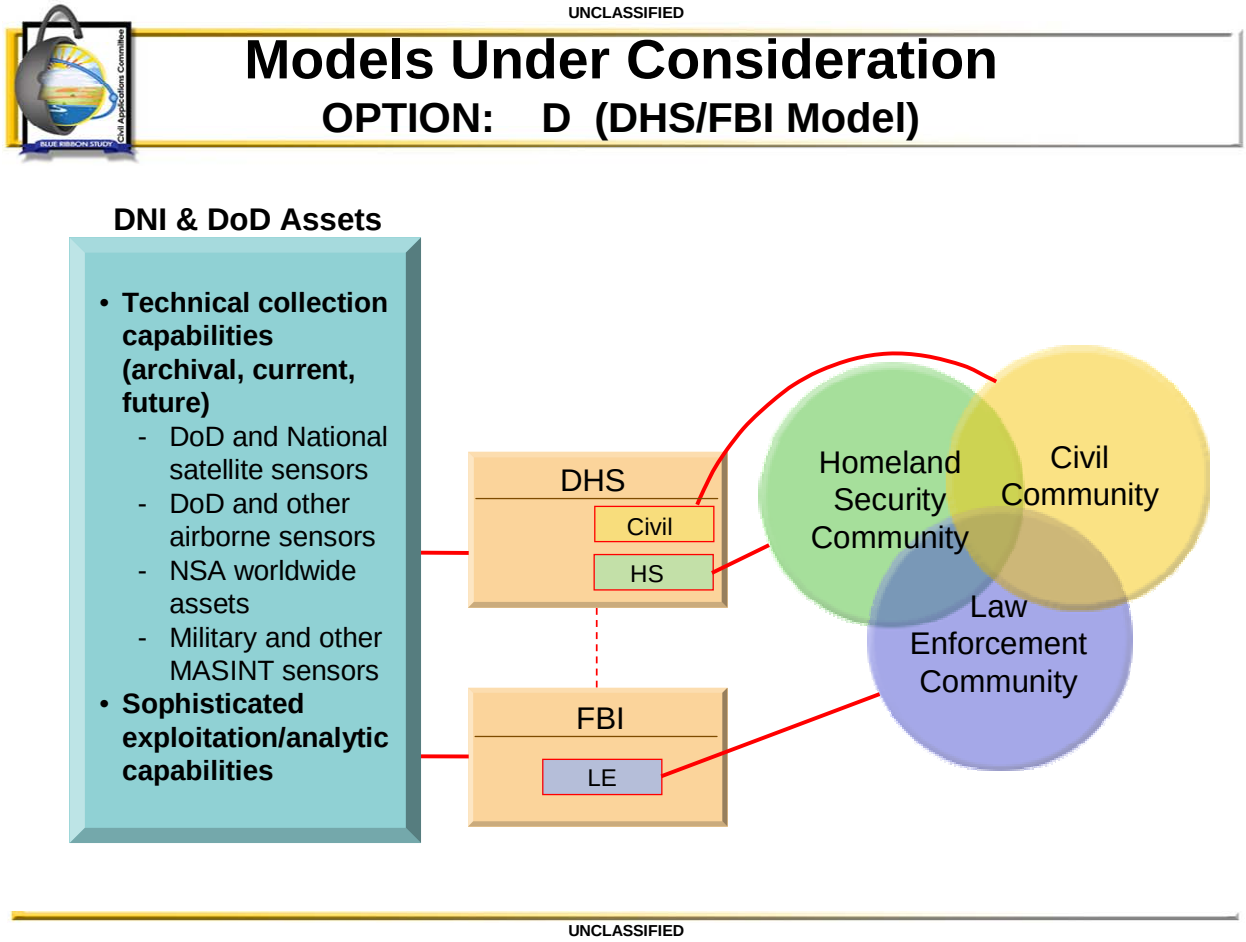

Figure 10.

The final model was a distributed model (**Figure 11**). Each of the domains had their own focal point for access into the IC. Since this model requires: start-up funding for three separate processes; three processes each with its' own priorities; three budget sustainment process; and overall, presents a strong potential for duplication, this model was eliminated without debate. Also, this model presented a strong pre 9/11 image of non-integration and limited information sharing.

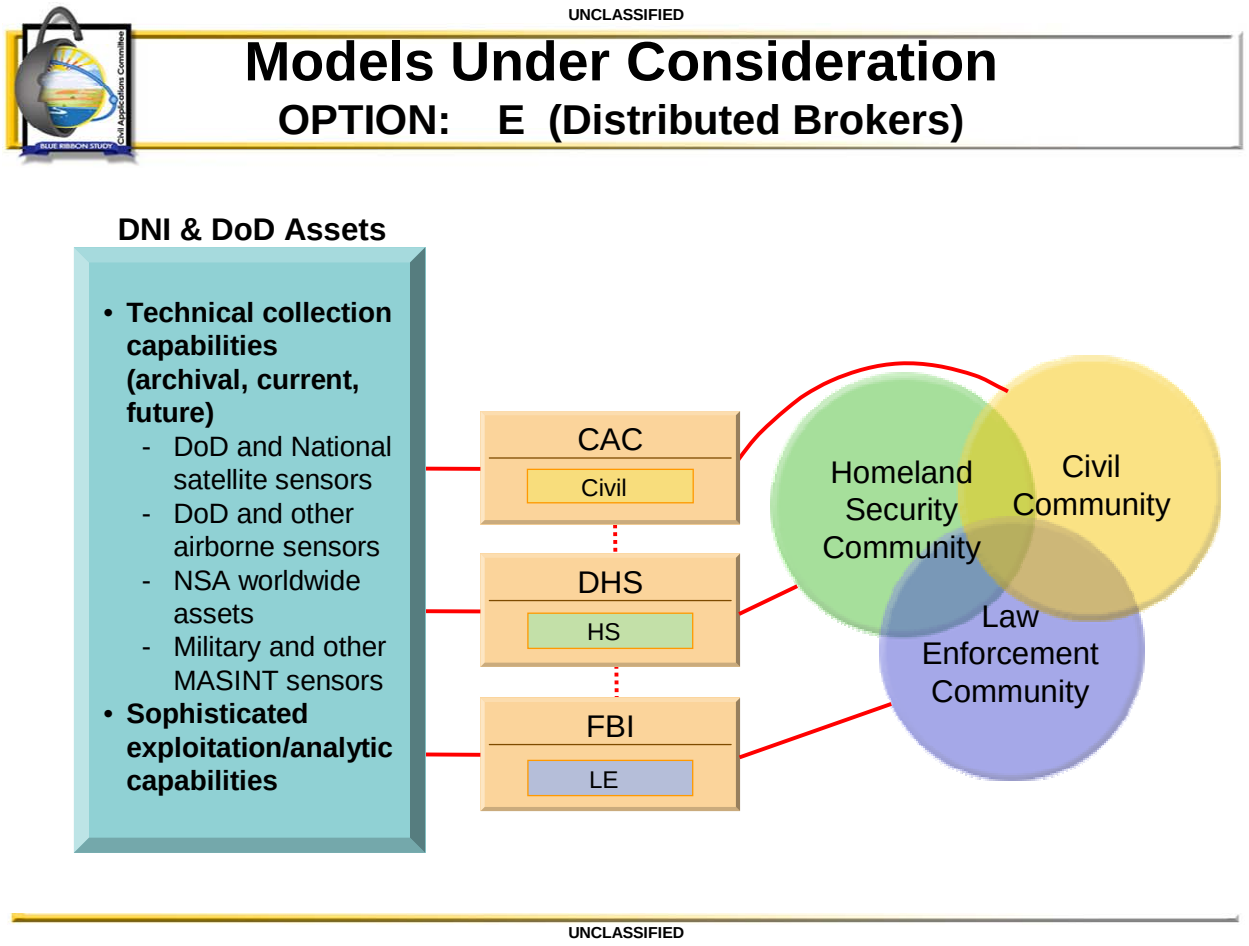

Figure 11.

CHAPTER 4: NEXT STEPS

Immediate:

The ISG believes the following actions need to be implemented to make an immediate impact on the country's ability to support domestic applications of IC capabilities:

- DNI approve ISG plan to improve support the domestic community.
- Establish an Executive Agent agreement between DNI and DHS to establish the Domestic Applications Office.
- DNI appoint an Implementation Program Manager (Senior Executive or Flag rank) to ensure successful transition to a new paradigm.
- DOJ, DNI and DOD jointly establish a legal fast track decision process to provide guidance regarding domestic applications of IC capabilities.

- DNI update policy directives relating to the use of IC capabilities for domestic uses. An important precept of the new guidance would be a program of risk management focusing on sharing of information and addressing technical collection capabilities legal limitations while at the same time protecting the civil liberties of U.S. persons.
- DNI address the issue of release of literal IDPs at .5 meter resolution and declassifying NTM at the .5 meter resolution.
- DNI address the issue of "ownership of information" which is hampering the sharing of information for the successful execution of Agency missions.
- The Department of Interior undertake a 90 day effort to compile a master list of government remote sensing holdings.

Near Term:

The following additional actions, implemented with in the next 12 months, will put in place a robust, viable program:

***DNI Actions*:**

- Create an FY 06 funding line for the Domestic Applications Program to include people, program dollars and seed money for a Domestic Exploitation of National Capabilities Program. Ensure current capabilities address support to domestic user needs.
- DNI should delegate authority to the D/NGA over domestic imagery tasking, exploitation, retention and dissemination.
- Work with DHS to establish the Domestic Applications Executive Committee.
- Establish a training and education program for customers to better understand how IC capabilities may be applied in a domestic environment.
- DNI add Domestic Community representative to the Mission requirements board (MRB).

***DHS Actions*:**

- Create a Domestic Applications Implementation Team.
- Stand up the Domestic Applications Office within one year.
- Determine how DHS unique information sharing authorities can facilitate the use of IC capabilities in the domestic context.
- Work in parallel with the CAC for one year or as mutually agreed to before accepting full civil domain responsibilities.

***CAC Actions*:**

- Work in parallel with DHS for one year to ensure a seamless transition.
- Migrate the CAC to the Civil Domain Working Group after one year.

***General Actions*:**

- Amend E.O. 12333 to articulate national policy on the domestic use of IC capabilities particularly in support of homeland security and law enforcement.
- Amend E.O. 12333 to provide for the oversight of domestic uses of IC capabilities by the Privacy and Civil Liberties Oversight Board.