Pre-Hearing Questions for Ms. Priscilla Guthrie,
Nominee for Chief Information Officer of the Intelligence Community

Commitment to Respond to Congress

1. For any of the following questions to which you are not yet able to provide detailed responses, will you commit to Congress to provide the responses within six months of taking office?

   Yes.

Prior Experience

2. Please describe the scope of your responsibilities as Director of the Information Technology and Systems Division at the Institute for Defense Analyses; Deputy Assistant Secretary of Defense (Deputy Chief Information Officer) at the Department of Defense; Vice President of TRW, Inc.; and as a member of the Strategy Advisory Group for US Strategic Command.
   a. For each position, please provide the approximate size of your offices in terms of employees, contractors, budget, and other resources.
   b. For each position, please describe your most significant accomplishments.
   c. If applicable, for each position, please describe the specific actions you took to improve information sharing, information security, and collaboration.

   <u>Director, Information Technology and Systems Division, Institute for Defense Analyses</u>

   Manpower/Resources: 57 employees, with approximately 20 subcontractors, and 30 consultants. Budget is approximately $18 million/year in expenditures.

   Significant Accomplishments: We increased support to DoD and DNI sponsors in assured information sharing; defining and implementing enterprise infrastructures to support assured information sharing; and cyberspace operations, including supply chain risk management.

   Specific Actions:

   - Rewrote the Division mission/vision/strategy to focus on cyberspace operations.
   - With the leadership team, I debated and developed perspectives on key sponsor challenges, including architecture and data. I used the ideas/products to assist government sponsors.
   - I vectored the research program to address topics of interest to sponsors, such as federating registries to support enterprise-wide discovery and access to services and data, including security services.

- I personally led several tasks focused on information sharing for government sponsors.

Deputy Assistant Secretary of Defense (Deputy Chief Information Officer), Department of Defense

Manpower/Resources: 90 employees, 110 contractors. Budget was $10 - $18 million/year. I supported CIO oversight of the $30 billion DoD IT budget.

Significant Accomplishments: I worked closely with DISA leadership to define and implement an enterprise, fiber, IP backbone. The program (GIG-BWE) was implemented on schedule and within budget. I led the focus on data, including the separation of data from applications, and drove the development of the DoD Data Strategy (to make data visible, accessible and understandable). I initiated the move to a services-based environment. I successfully advocated for the development of the DoD's information assurance architecture (NSA product: IA Component of the GIG Architecture).

Specific Actions:

- I reorganized to focus key resources on data and information sharing. I personally led the resulting new unit during start-up to highlight the importance and provide time to recruit the right director.
- I worked closely with DISA and NSA, pushing both organizations beyond their comfort level to build the base for assured information sharing.
- I sponsored the Horizontal Fusion portfolio. The resulting capabilities were based on the new DoD net-centric vision/strategy and were deployed to Iraq and Afghanistan with XVIII Airborne Corps to support operational requirements.
- I worked closely with allies on policies for information sharing in-theater.

Vice President and General Manager Commercial Market Area and VP E-Business, TRW Inc.

Manpower/Resources:

- Commercial Market Area: P&L with approximately 2,500 employees in 13 countries and $500 million/year sales.
- E-Business: Small unit (approximately 25 personnel) reporting to CEO of $17 billion company. Budget was approximately $20 million.

Significant Accomplishments:

- Commercial Market Area: I restructured acquired businesses into a profitable $500 million+ unit delivering IT services and solutions to customers in the Manufacturing, Public Safety Systems, Healthcare and Human Services sectors.
- E-Business: I established and led a small, global unit responsible for driving new IT technologies into the $17 billion company's businesses to create competitive

advantage. I optimized business processes, including the integration of a $7 billion acquisition.

Specific Actions:

- Commercial Market Area: I sold or closed units and businesses that were not profitable and/or that were not aligned with the strategy we developed for the new organization. I organized along market sectors and leveraged company competencies in IT and manufacturing.
- E-Business: Designed and implemented customer/supplier portals. Piloted supply chain tools and processes to optimize operations. Fielded collaborative design and engineering tools and "follow-the-sun" distributed processes. Updated the IT security policy, and developed and implemented a company web-site.

Member, Strategic Advisory Group (SAG), USSTRATCOM

Manpower/Resources: Chair of the Cyber Panel and member of the C2IS Panel. The Cyber Panel consists of approximately 20 members and advisors.

Significant Accomplishments:

- I provided advice to Commander, USSTRATCOM, as requested. Other recent tasks included: chaired a Nuclear Command and Control Review, supported an interagency cyber limited objected experiment as a senior mentor, and chaired a review of Global Sensor Integration activities.

3. What specific experience have you had either working with the Intelligence Community (IC) or in resolving intelligence-related issues?

   I worked with the Defense Intelligence agencies as part of the Department of Defense (DoD) Communications, Command, Control, and Intelligence (C3I) organization from 2001 to 2004. From 2003 – 2006, I worked closely with the National Security Agency (NSA) on the development of a security architecture for the enterprise information environment (Information Assurance Component of the Global Information Grid Architecture). I chair the Cyber Panel for the USSTRATCOM Strategic Advisory Group (SAG). Cyber is one of USSTRATCOM's three primary missions. The Cyber Panel provides advice to the Commander, USSTRATCOM on topics of interest such as forces, effects, and deterrence. I supported a Defense Science Board Task Force in developing a report on "Integrating Sensor-Collected Intelligence." In my current position, I am responsible for two tasks that support the ODNI and several tasks that focus on cyber operations. As part of my work on the USSTRATCOM SAG, I also recently chaired a Nuclear Command and Control (NC2) review in support of the NSA Advisory Board.

4. Based on your experience, to what extent does the IC present unique challenges for the development and management of activities related to information technology (IT) and enterprise architecture requirements?

The composition of the Intelligence Community (IC), where the majority of the IC elements also fall under other Executive Branch Departments with their own policies, processes, and priorities (such as Defense, Treasury, Homeland Security, State, Justice, etc.,) creates unique challenges in the integration of the architecture requirements and information technology of the IC with those mandated by the element's Department. Conflicts arise as a result of each IC element's special security requirements, the diverse customer bases, and the unique mission requirements of each element and Cabinet Department. With the establishment of the ODNI and information sharing and integration mandates in IRTPA, the IC CIO is leading the transition to an information sharing culture by providing the plans, policies, standards, services, and oversight to support the transition. The lack of clear IC lines of authority complicates the management of IT activities. The IC is working with other Executive Branch Departments to adopt common standards and develop an architecture that enables interoperability.

5. Based on your private sector experience and your understanding of the IC, please estimate, based on industry norms and/or trends, what percentage of the total National Intelligence Program (NIP) and Military Intelligence Program (MIP) budget is likely to be, and should be, devoted to IT information systems. Based on these observations of the public sector, what accounts for differences between the amount of IT funding between the public and private sectors, and what problems does that present?

   While it is always useful to benchmark other organizations, and to leverage applicable best practices, I do not believe it makes sense to apply an industry norm to IC IT budgeting. The scale, acquisition regulations, oversight and governance processes, and mission make government different from industry. Return on investment is relatively easy to compute in industry while it can be problematic in government, especially when the primary product is information – a product that can be hard to value in monetary terms.

6. To the extent possible, please provide specific examples from your past experience of how you effected major change over the opposition of others over whom you had little or no direct authority.

   As the Deputy DoD CIO, I felt that the Department's net-centric vision would not work without revised approaches to data, information assurance and architecture, and I needed the support of DISA, NSA, the military departments and others to implement the necessary changes. Under my leadership, the Department developed and approved the DoD Data Strategy, and initiated the move to a services-based information environment. A comprehensive information assurance component of the architecture was developed by NSA and approved. These policies provide architectural foundation for DoD IT and are also used in the oversight and governance processes to force compliance.

   As the Vice President of E-Business for TRW, my team led the optimization of business processes and the selection of product development and supply chain products for the company. To implement these changes, we invited staff from the business units to participate throughout the process redesign and product selection processes. The decisions were business- vice consensus-based, so we worked closely with the CEO and Finance to track progress and enforce compliance.

7. To the extent possible, please provide examples of decisions made by you and executed by the organization that were widely perceived as unpopular. For each example, please explain why you made that decision, how you overcame opposition, and what actions you took to make the decision more widely accepted.

   As the Deputy DoD CIO, I eliminated a directorate focused on e-business and created a directorate focused on data. Eliminating the directorate wasn't popular with employees or with affected agencies, and data wasn't perceived to be an appropriate topic for a DoD-level directorate. By handpicking the new directorate personnel and by personally leading the new organization, I signaled its importance. I took the time to select a strong leader to replace me. We spent considerable time briefing others on the importance of data to the Department's vision for net-centric operations. This unit produced the DoD Data Strategy.

   As the Director of Operations for TRW's Automotive Aftermarket, I restructured and streamlined operations, closing marginal facilities, eliminating central warehousing and private trucking, and ending union relationships that weren't mutually advantageous. I led the implementation of pass-through packaging and distribution across North America, and we earned a best-in-class from two top automakers; I also globalized purchasing where it made sense. At first, employees were concerned about loss of jobs, especially highly paid, blue-collar employees. By selecting top performers for key positions, offering training for the best employees, and showing that we could increase the bottom line and order fill for customers, I gained support for the changes. We sold the business – it was one of the company's most profitable sales and included a long-term supply contract.

   As the Vice President and General Manager of the Commercial Market Area for TRW, I wanted to settle lawsuits that the company inherited as part of a $1billion acquisition. Company management was initially not supportive for a variety of reasons. Employees from the acquired unit were opposed, as they believed the issues could be fixed. I made the decision to settle after reviewing the cases with the legal staff. I didn't think additional effort would help the former customers of the acquired company – it was too late, and I believed that we needed our key resources focused on building the new organization. I sold my approach to management and focused my energy on working with existing and new customers and with the employees of the new organization.

Duties of the Chief Information Officer of the IC within the Office of the Director of National Intelligence

8. What is your understanding of the duties and responsibilities of the Chief Information Officer (CIO) of the IC? Have you discussed with the Director of National Intelligence (DNI) his expectations of the IC CIO?

   The duties and responsibilities of the IC CIO are as defined by statute and in accordance with policy established by the DNI in various intelligence community policy documents. The DNI has broad statutory authority, some exercised through the IC CIO, for the development of an integrated, interoperable and interdependent information technology infrastructure across the intelligence community enterprise. The DNI has principal authority for

intelligence community information sharing, to ensure maximum availability of and access to intelligence information consistent with national security requirements. In the exercise of this statutory responsibility, the DNI is charged by law with the duty to establish common information technology standards, protocols and interfaces across the IC, to ensure the development of IT that includes multi-level security and intelligence integration capabilities, and to develop an enterprise architecture for the IC. The DNI is also responsible for ensuring that elements of the IC comply with that architecture. Per Intelligence Community Directive (ICD) 500, the DNI has authorized the IC CIO to perform duties on his behalf. In support of these efforts, the IC CIO, subject to the direction of the DNI, also has the statutory responsibility to direct and manage all IT related procurement for the IC, and to manage activities relating to the IT infrastructure and enterprise (EA) requirements of the IC. The IC CIO also has, by statute, procurement approval authority over all IT-related procurement for the IC and, per ICD 500, is to be informed of any agency-specific decisions, as he or she deems appropriate. If confirmed, I will work with the DNI to understand his direction and guidance with respect to IC IT activity within the IC elements as described in ICD 500. With respect to IT support for information sharing, in ICD 501, the DNI has directed the IC CIO to develop the IT architecture that supports the information sharing policies and objectives laid out in the Directive, and to develop and promulgate standards to support the directive in accordance with established ODNI processes.

The DNI discussed the basics with me when he asked me to consider this assignment. If confirmed, I will work with the DNI to understand his direction and guidance.

9. What do you perceive as the greatest challenges facing the CIO of the IC?

From my current vantage point, the greatest challenges for the IC CIO appear to be:

- Enabling the intelligence mission by facilitating information sharing among authorized users while protecting both the information and the information environment;
- Developing and implementing an architecture to support the varied IC user requirements;
- Establishing policies and governance processes to drive implementation;
- Building a workforce capable of leveraging information resources and aware of their responsibilities for maintaining these resources; and
- Maintaining public trust.

10. The IC CIO's statutory duties and responsibilities include managing "activities relating to the information technology and enterprise architecture requirements of the Intelligence Community."
    a. If confirmed as IC CIO, how do you plan to establish architecture requirements for intelligence components in the various departments of the federal government, in particular the Central Intelligence Agency (CIA), Department of Defense

(DoD), Federal Bureau of Investigation (FBI), and the Department of Homeland Security (DHS)?

If confirmed as the IC CIO, my role will be to establish a vision for the IC that is understood within the IC agencies/elements, and by their operators, policy-makers and technologists. This vision will be the basis for establishing architectural requirements that enable collaboration and information sharing across the community in support of the mission.

b. How do you intend to deal with intelligence agencies within the various departments, which may have conflicting guidance on enterprise architecture requirements?

It is my understanding that the Intelligence Reform and Terrorism Prevention Act provides the DNI the authorities to unify guidance across the IC. It is the IC CIO's role to encourage and enforce combined action bringing together the strengths of the IC elements through enterprise architecture. Resolving conflicts is a normal part of architecture development and is part of every CIO's job.

c. Will you commit to keeping Congressional oversight committees fully and currently informed of any significant conflicts with these intelligence agencies and their resolution?

If confirmed, I will keep the Committees fully and currently informed of any significant conflicts with these intelligence agencies and their resolution.

11. If confirmed as the IC CIO, how do you plan to work with the IC's Civil Liberties Protection Officer to ensure that "the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information" as required in section 103D of the Intelligence Reform and Terrorism Protection Act of 2004 (IRTPA)?

If confirmed, I will work to enhance the level of privacy awareness, training, and expertise among CIO staff across the community so that they have subject matter expertise required to ensure privacy compliance in developing and operating information technology environments, and in conducting information-sharing activities.

If confirmed, I will work with civil liberties professionals to ensure they are aware of information technology projects at the earliest stages, so that privacy protections can be built-in from the start.

12. If confirmed as the IC CIO, how would you propose to integrate IC centers, such as the National Counterterrorism Center, and the information they process, analyze and disseminate, into an overall IC enterprise architecture? What, if any, do you see as information management challenges associated with the operation of these national intelligence centers?

I have not had an opportunity to engage with any IC center management or staff, however from my current vantage point, I see a need to ensure that all of the IC centers understand and comply with CIO policies. The key information management challenges appear to be lack of: an enterprise architecture and infrastructure; information assurance policies and enterprise tools to enable the policies; and necessary enterprise governance policies and processes.

Accountability and Effectiveness

13. In 2004, Congress and the President created the position of the DNI in large part due to the ambiguous authorities of the former Director of Central Intelligence (DCI). These ambiguities forced prior DCIs to manage the IC through consensus rather than dictating certain outcomes. Some criticism has been levied against the first two DNIs that they, too, managed the IC by consensus, despite the added authorities granted by the IRTPA. It remains to be seen how the current DNI will use his authorities.
    a. Do you believe that the authorities granted to the IC CIO by statute, Executive Order, and IC Directives are clear and powerful enough to direct the full integration of IC information sharing systems regardless of the leadership style of the DNI?

I understand that the current IC CIO authorities contain some overlap and ambiguity with respect to other related laws and policies that may attenuate the authority of the IC CIO. If confirmed, I will work with the DNI, the Community, and the Committee to clarify ambiguities while fully exercising all authorities prescribed in legislation.

    b. If confirmed as the IC CIO, do you intend to lead through consensus-building or will you be more directive?

If confirmed, I will use all authorities granted by statute and policy. As shown in my response to Question 7, I have no qualms about using my authority. However, consensus building is one of the many tools the IC CIO will need to use in order to meet the underlying goals of the position's authorities. Specifically, most elements of the IC are part of other, independent departments and agencies, which exercise statutory authority for IT independently of the IC CIO or the DNI. The IC is neither a department or an agency, and other statutes, such as FISMA, Title 10, and the Clinger-Cohen Act of 1996 (Title 40), provide agency heads with authority over IT within their agencies. Moreover, I understand that the abrogation clauses in IRTPA and in Executive Order 12333 may also generate some uncertainties. I believe that reconciling the implementation and execution of these overlapping authorities will require collaboration and coordination, team building, unified vision, and consensus leadership.

Authorities of the CIO of the IC

14. What tangible metrics and milestones do you believe Congress should use to measure your progress in creating a secure enterprise architecture which facilitates the kind of information

access envisioned by the 9/11 Commission and the DNI's "Vision 2015: A Globally Networked and Integrated Intelligence Enterprise", published July 22, 2008? How should Congress use such metrics and milestones to hold you and the Office of the DNI accountable for progress, or lack thereof? Will you commit to present to Congress a list of these metrics and associated timelines within six months of taking office?

I believe the IC CIO must establish a robust, secure information environment that enables authorized users to discover and retrieve the information they need, when they need it, and in a form that is useful and supports their mission requirements. If confirmed, I will provide metrics and associated timelines that Congress will be able to use to assess progress.

15. Please describe your understanding of the interactions between the IC CIO and each of the following: Information Sharing Environment Program Manager; Associate Deputy DNI for Information Integration; IC agency CIOs; Departmental CIOs; the NRO's Ground Enterprise Directorate; and the functional managers for the various intelligence disciplines. Please identify areas of overlapping responsibilities, the IT-related activities, and how you intend to leverage each as an asset.

    The ISE-PM supports counterterrorism information sharing across the government. It is my understanding that the IC CIO's interface to the ISE-PM is similar to the interfaces between the ISE-PM and the Departmental CIOs.

    The IC CIO function was reorganized by the DNI in May 2009 to clarify lines of authority. The ADDNI for Information Integration has been disestablished and that organization now reports to the IC CIO. Additionally, it is my understanding the IC CIO and the DoD CIO have established a partnership and have a list of more than 40 initiatives they cooperatively execute, from standards development to joint policy efforts.

16. Please explain the DNI's authority to formulate, implement, and enforce IC-wide information access policies, including those policies related to the development of an information sharing environment and whether the recent modifications to Executive Order 12333 have sufficiently established a framework to enable the IC to operate like a true "information enterprise" where information is accessible by all IC elements.

    The IRTPA and the amended EO 12333 give the DNI authorities for information sharing. I've reviewed ICD 501, the new policy for information discovery and access within the IC. The framework described in the ICD, where analysts and collectors can "discover" information without being given access to the content, with follow-up procedures for granting appropriate access to the content, is a concept that has been championed by information sharing studies, including the Markle Foundation study. If confirmed, I'll work to develop and implement an IT infrastructure to enable these concepts. Issues with authorities are discussed in the answers to Questions 8 and 14.

17. What additional modifications to Executive Orders, statute, or relevant policies and directives do you believe should be made to facilitate the IC operating like an "information enterprise?"

As to statute, it is my understanding that the Administration's intelligence authorization proposal for Fiscal Year 2010 is in the final stages of coordination. I understand that this proposal contains provisions to enhance the authorities of the DNI to manage the intelligence community. If confirmed, I will review this proposal carefully and if I see a need for additional legislative authorities, I will not hesitate to ask for them. With respect to Executive Orders and policies, if confirmed, I will seek to involve myself in all policy reviews relevant to the duties of the IC CIO and make recommendations for modification, as necessary.

If confirmed, I will assess the existing Executive Orders, statutes, policies and directives to see how they support the CIO in integrating and operating the IC as an "information enterprise" and I will work with Congress to address any required additions and /or modifications.

18. Have you reviewed the relevant memoranda of agreement between the ODNI and the DoD relating to authorities over jointly funded (using both NIP and MIP funds) programs? If so, do you foresee any problems with these arrangements? For example, the Distributed Common Ground System is funded by the DoD. How do you plan to fully integrate that critical IT architecture(s) with the IC enterprise?

I have not had the opportunity to review the MOA between DNI and DoD regarding authorities over jointly funded programs. However, I am aware that the ODNI/Chief Financial Office is leading a review of NIP/MIP issues in coordination with the Under Secretary for Intelligence (USD(I)). If I am confirmed, I will engage within ODNI and DoD to ensure that we are fully exercising DNI authorities in concert with our partners in DoD to ensure the integration of DCGS and the IC enterprise architecture. I envision integration at the information level through common data standards and the reuse of IT services where applicable.

19. Intelligence Community Directive-501 (ICD-501), "Discovery and Dissemination or Retrieval of Information within the Intelligence Community," directs the IC CIO to accomplish a number of tasks relating to the development and promulgation of standards. To the best of your knowledge, do these standards exist? Have they been promulgated? If confirmed as the IC CIO, how will you use your authorities to *enforce* the standards vice simply promulgating them?

It is my understanding that the information sharing construct established by ICD 501 relies on existing standards. New standards are likely to be required to facilitate the discovery and retrieval of information. If confirmed, I will communicate with the IC leadership to ensure that they understand the vision, strategy and standards, and the need for organizational compliance. Governance processes must be established to enforce compliance. This must be a CIO priority.

20. Section 102A(g)(1)(F) of the National Security Act of 1947, as amended, provides the DNI "procurement approval authority over all enterprise architecture-related information technology items *funded in the National Intelligence Program*." However, section 103G(c) states that "Subject to the direction of the [DNI], the [CIO] shall . . . (2) have procurement

authority over all information technology items related to enterprise architectures *of all intelligence community components*." How do you interpret these authorities? In your opinion, do they extend to all IC components or just those program elements funded by the NIP?

The DNI's authority seems to be limited to the NIP, while the IC CIO's authority appears to extend more broadly, yet it is subject to the direction of the DNI. This creates some ambiguity. However, since the CIO's authority is subject to the direction of the DNI in either case, if confirmed, I will seek the guidance of the DNI in carrying out the CIO responsibilities, and I will work with the Committee to clarify ambiguities.

21. Section 103G(c) of the National Security Act of 1947, as amended, states: "Subject to the direction of the [DNI], the [CIO] shall . . . "

    a. How do you interpret that caveat as it pertains to your authorities?

I interpret this statement to mean that the IC CIO reports to the DNI, and that the exercise by the IC CIO of the authorities listed in that statute are to be carried out under the direction of the DNI. Day-to-day, I would expect this to mean that the CIO's actions must be in coordination and consistent with the direction of the DNI.

    b. Do you consider ICD-500 to be the referenced direction of the DNI?

Yes. I will seek the DNI's guidance on any issues that impact my ability to meet mission requirements.

    c. If so, how do you interpret the DNI's direction in ICD-500, paragraph 1, to "coordinate with" IC agencies and departments to "produce compatible architectures, and common standards and policies ensuring the greatest transparency for intelligence support"?

If confirmed, I will discuss this issue with the DNI so that I understand his intent.

    d. Do you believe the DNI's direction to merely coordinate with agencies reduces your effective leverage over them? If not, please cite the exact provision that you believe provides you more than the authority to be a coordinating influence.

If confirmed, I will ask the DNI about his intent and for his direction, and consult with the Committee if any legislative action is required.

22. The previous IC CIO was told by certain IC elements that he only had influence over their "enterprise" IT systems and not the "mission" IT systems. Please explain how you, if confirmed as the IC CIO, would deal with an IC element telling you that one of their IT systems cannot be "micromanaged" by ODNI staff.

If I am told, as the IC CIO, that I cannot influence the IT activities of the IC elements in accordance with my authorities, I will not hesitate to elevate the discussion until there is an acceptable resolution, consistent with the mission and authorities of the IC CIO and of the DNI. I expect there will be issues since ICD 500 allows IC agency heads to make procurement and acquisition decisions regarding exclusively internal agency systems designed to facilitate the conduct of agency operations and activities. It strikes a delicate balance, ensuring that the IC CIO may exercise his or her authorities to ensure that the IC's IT architecture is implemented across the IC, while recognizing that the IC CIO need not participate in every internal agency procurement.

Leveraging Commercial Best Practices

23. If confirmed as the IC CIO, what will you do to leverage commercial IT capabilities for use in the IC?

    I have been informed that most of the IT capabilities within the IC are based on commercial technologies. While commercial technologies can offer significant advantages that should be leveraged, such as robust user support and market pricing, there are also potential downsides, such as the security of products that may have been developed in countries with interests that are counter to ours. The trade-offs must be evaluated. This is part of every CIO's function.

24. If confirmed as the IC CIO, how will you leverage the cloud architecture work being developed by several leading commercial IT firms?

    Cloud computing technology has great potential to advance mission capabilities. Cloud computing presents opportunities for rapid discovery and access to information collected and produced by the IC. One of the challenges in the commercial sector and the IC is the protection of information in the cloud. If confirmed, I will seek to leverage the opportunities presented by cloud computing to improve information sharing while protecting these resources.

25. Companies like Google were developed to aggregate large numbers of datasets and make them available to users using straightforward open standards. If confirmed as the IC CIO, how will you aggregate the data collected by the DNI and the IC to make sure it is readily available to the users?

    Ensuring availability and access to information is a shared responsibility across the IC. I understand the IC uses commercial technologies like Google to deal with large datasets. The success of Google and other search engines is due in part to the fact that companies and people want their information to be easily discovered. They can and do revamp web pages and legacy systems to improve visibility and increase the number of "hits" on their websites. Legacy IC systems often were built to keep secrets and prevent discovery. If confirmed, I will develop and implement policies to achieve assured information sharing.

26. Do you believe the U.S. business community is equipped to serve the needs of the CIO of the IC? If confirmed, how would you utilize the services of the business community to fulfill the mission of the office? What strategies would you adopt to ensure the business community provides value to the IC at a reasonable price?

I believe maintaining an open dialogue with the business community is essential to ensure that U.S. firms are prepared to provide the required IT services and products at a reasonable price, and to help the IC understand the market for IT products and services. The implementation of an IC Enterprise Software Licensing process across the IC is an important step toward achieving this outcome. I understand that last year, the ODNI and DoD jointly agreed to develop DoD and IC-wide Enterprise License Agreements for purchase of commercial software licenses. This initiative is designed to provide IC components with negotiated options for acquiring common, standards-compliant, and commercially available software under the most favorable terms and conditions by leveraging the purchasing power of a combined DoD-IC community. If confirmed, I intend to continue the outreach to the commercial community.

27. Do you believe that government CIOs should have to drive out costs from IT architectures in the same way private sector CIOs do? If so, what metrics would you apply to gauge their success in this regard?

Government CIOs are responsible for driving out costs wherever possible. Government CIOs must also put mission requirements at the top of their priority lists. It is not straightforward to maintain the appropriate balance between these often conflicting priorities especially within the IC; ROI calculations do not work well when the primary product is information. If confirmed, I will develop and share metrics for success with the Committee.

28. What are your thoughts about licensing agreements such as "pay as you use"? If confirmed as the IC CIO, would you support the use of such licensing agreements across the IC?

"Pay as you use," and lease services are relatively new concepts with evolving business models. Lease versus buy decisions must be made with comprehensive knowledge of terms and conditions, agility, costs, and rights. For national security reasons, the IC may have issues making its usage statistics available to support required payment agreements. If confirmed as IC CIO, I will address these issues in the context of the larger goal of improving enterprise-level efficiencies, managing and reducing cost, and maximizing mission effectiveness. At a minimum, I will investigate partnering with Government Departments, such as DoD, which has established a successful enterprise software licensing program--the Enterprise Software Initiative--to address IC requirements.

Vision for an IC Enterprise Architecture

29. What is your general assessment as to how well the IC is sharing information and/or collaborating over seven years after the 9/11 terrorist attacks?

I have been told the Intelligence Community has made great progress in sharing information and collaborating since the 9/11 terrorist attacks. I also understand the IC continues to identify ways to improve information sharing and collaboration, including the recent promulgation of ICD 501, *Discovery and Dissemination or Retrieval of Information within the Intelligence Community*.

a. Is the IC striking the right balance between sharing information and protecting sources and methods?

It is my understanding that the IC is moving forward on both fronts but I do not have enough information to judge the balance. If confirmed, I will consult with the DNI and IC leadership to strike the right balance between sharing information and protecting sources and methods.

b. Do you believe an "originator control" approach is still in effect within the IC? If so, should it be?

It is my understanding that "Originator Controlled" is still in effect within the IC and in other parts of the government.

c. To what degree are agencies resisting change in the area of information sharing? If they are resisting, to what extent are they doing so by exploiting ambiguities that exist in the IRTPA and any prior law? Please cite any specific instances of these ambiguities.

I have not had the opportunity to review specifics regarding agencies' resistance to change in this area. If confirmed, I will assess progress and challenges in this area, and chart a course of action.

30. Has the IC instituted adequate technical and organizational mechanisms for policy compliance, oversight, and dispute resolution in the area of information management? If not, what more must be done in this area?

It is my understanding the IC CIO oversees IC IT procurements, participates in the development of planning and programming guidance through the IC Strategic Enterprise Management process, and oversees budget development for National Intelligence Program IT components. Using an IC IT Portfolio Management process, the CIO leads reviews, assessments, and prioritization of IT investments. These efforts are designed to identify and eliminate parallel, redundant, or stove-piped systems, and focus IT resources on intelligence priorities. Still, I do not have enough information to determine whether the mechanisms are adequate. If confirmed, I will assess the adequacy of the technical and organizational mechanisms.

31. The FBI's IT problems have been widely discussed in Congress and the media.
    a. What lessons do you believe should be learned from the FBI's experience?

b. Based on your understanding of information available to you, is the FBI now on the right track?
c. If confirmed, what role do you expect to have in the future development of the FBI's IT and enterprise architecture requirements?

If confirmed, I will review the IT portfolios of the IC components, including the FBI.

32. As you may be aware, many state and local government organizations have established "fusion centers" for various purposes.
    a. How, if at all, do you see these centers being integrated with the ODNI, US Northern Command, the FBI-led Joint Terrorism Task Forces, the Department of Homeland Security's intelligence activities, and the broader IC?
    b. What significant legal, policy, and resource issues do you believe are involved in such integration?

I am aware of the existence of state, local, and regional Fusion Centers and understand that they are all different, but do not have enough information to make any assessments.

33. In general, what consideration should be given in the development of IC enterprise architectures to permit real-time access, at appropriate classification levels, by state and local officials to intelligence information?

If confirmed, I will work to develop an enterprise information environment that leverages access controls and cross-domain guards as part of a robust information assurance capability that enables assured information sharing.

34. Some of the information needed by intelligence analysts and their customers is unclassified, open-source information. How do you believe open-source information should be handled within the IC's enterprise architecture?

I believe open-source intelligence should be an integral part of the IC information environment.

35. If confirmed, how would you manage, and what priority would you give to addressing the following issues:
    a. the protection of the privacy interests of U.S. persons;
    b. the vulnerability of IC information systems to harm or espionage by trusted insiders;
    c. the vulnerability of IC information systems to outside penetration;
    d. the readiness of IC components to maintain continuity of operations;
    e. the IC's ability to adopt advanced information technology efficiently and effectively; and
    f. the IC's recruitment and retention of skilled information technology professionals.

I believe the IC must remain fully committed to continuing the protection of the privacy interests of U.S. persons, including compliance with the Privacy Act of 1974, the E-

Government Act of 2002 and working closely with privacy and civil liberties experts. If confirmed, I will ensure the Civil Liberties Protection Officer has visibility into IC CIO processes and resources containing personal and privacy information.

The IC CIO should work with the National Counterintelligence Executive (NCIX) and other IC counterintelligence components as necessary in assessing the vulnerabilities of our information systems.

The IC CIO role includes the responsibility to work across the IC, industry, and academia to identify, pilot, and implement emerging technologies. Throughout my career, I have tracked industry trends, best practices and future technologies. If confirmed, I plan to incorporate this practice within the "build to" plans of the enterprise architecture and the strategy for piloting new capabilities to meet emerging community needs.

I'm told the office of the IC CIO, working with the IC Chief Human Capital Officer, has a professional development program to ensure IT professionals retain leading edge skills and remain savvy consumers of technology and services. Recruiting is another critical component in building a professional cadre.

36. If confirmed, what would be your priorities with respect to the staffing of the Office of the CIO? How many employees do you anticipate being necessary for the Office of the CIO? What skills do you believe are most important for such employees to have? In light of your own DoD background, would you look for individuals with experience in law enforcement or the State Department?

If confirmed as the IC CIO, I will take the time to understand in detail the current capabilities of the Office of the Chief Information Officer (OCIO). Only then will I have sufficient information to determine what is needed to deliver required capabilities. The OCIO should be large enough to draw upon a breadth of IC experience, small enough to nimbly respond to changes in priorities, and sized to ensure accountability.

The most important skills are those which enable the OCIO to be a savvy consumer of services and skills. I would seek candidates with broad government. I'll also look for staff with experience and expertise in policy, technology and operations – diverse experience and expertise within the workforce is essential.

37. The IC currently operates on multiple networks, including NIPRNet, SIPRNet, JWICS, CWE, NSANet, FBINet, and NGANet. Do you believe these systems are adequately interoperable? If not, what steps will you take to improve their interoperability if you are confirmed?

These environments do not appear to provide the enterprise information environment required by the community. If confirmed, I will assess the situation and develop a plan for achieving the required level of interoperability.

38. Please review the DNI's "Vision 2015: A Globally Networked and Integrated Intelligence Enterprise", published July 22, 2008, and the DNI's report to Congress "Implementing Vision 2015", submitted November 17, 2008.

a. Do you agree with the vision(s) described?

I believe that Vision 2015 presents a plausible picture of the future threat environment and an appropriate target for transformation of the IC.

b. If confirmed, how will you implement it given the obstacles which have stalled similar efforts?

Vision 2015 is the vision for the IC as a whole, not just the CIO's vision. Implementing this vision will require a concerted effort by the IC elements, leaders, and the workforce. The IC CIO can do its part in the Vision 2015 transformation by making information and services available to users to support their mission requirements.

c. What tangible milestones will you apply to implementing this vision?

I understand that some work has been accomplished in developing an information strategy and program plan. If confirmed I will review those products and establish milestones for implementing the vision, as appropriate.

d. What problems, if any, do you foresee in such implementation?

I expect there will be problems with ownership, resourcing, and security (need to know versus responsibility to provide). I will work with the DNI, the IC, and the Committee on specific issues, as required.

39. Please review the "Report of the Joint Defense Science Board / Intelligence Science Board Task Force on Integrating Sensor-Collected Intelligence", published in December, 2008.

a. Do you agree with the report's general conclusions and each of its recommendations?

I was a member of the task force that developed this report and I support the recommendations. The IC CIO has a role to play in establishing the architecture and standards to support making data and services visible, accessible and understandable. However, ICD 500 currently allows IC agencies/elements to decide what constitutes a mission system and to build such systems on their own. This could significantly limit the role of the IC CIO in implementing the recommendations in the Report.

b. Please explain, with specific descriptions if appropriate, how you would use the position of IC CIO to enact those recommendations with which you agree.

If confirmed, I will consult with the DNI on the extent of expected IC CIO engagement and move forward accordingly.

40. Vision 2015 and the joint Integrating Sensor-Collected Intelligence report advocate investment in processing, exploitation, and dissemination (PED) architectures. Other studies, initiatives, and IC seniors have made similar arguments, claiming that a better return on investment is found in "the ground" architectures. Do you agree with this? If so, will you advocate for greater resources for "the ground" even if this means fewer resources for sensors?

    I do not believe the ISCI report advocated a PED architecture. The report calls for data to be posted as soon as possible, a consumer-focused environment where the consumer pulls what he/she wants when they want it, which is quite different from a PED cycle where the producer exploits the data, then decides who should get it and when they get it.

    While sensors are important, the IC is experiencing diminishing returns analyzing the increasing volumes of data presently collected, restricting its ability to provide meaningful intelligence to customers. The IC must look at every situation carefully and weigh the costs and benefits of collection against the costs and benefits of increased ground processing or analytical support.

41. There has been a large push to accept prudent risk to declassify products to lower levels in order to increase information access. How would you see your role, if you are confirmed, in providing guidance on classification or declassification of products and/or raw intelligence data?

    If confirmed as the IC CIO, I will work to ensure that Intelligence Community IT supports efficient review of and access to information by appropriately cleared and authorized personnel.

42. Please review the August 2007 DNI study titled "Achieving a Robust Collaborative Environment." According to the August 13, 2008, report from the DNI OIG on "IC-Wide Integration and Collaboration Diagnostic and Recommendations," the 2007 study included 12 recommendations, but that as of August 2008, only one had been enacted. Please review the other 11 recommendations and identify those which you believe would be within your purview as CIO and whether or not you agree with the recommendations. If confirmed, how will you enact them?

    Recommendations 1-3: These call for the DNI to create a culture of collaboration, ensuring that business practices and infrastructure support collaboration, and setting an example for the community. The recommendations call on DNI and other IC senior leadership to "walk the talk" by exhibiting commitment to collaboration within their own organizations. The contribution of the IC CIO in this arena, therefore, is to set an example, to use collaborative tools and practices personally and to encourage and facilitate their use in the day-to-day operations of the organization. The DNI will require the expertise of the CIO staff in understanding what capabilities could be available.

    Recommendation 4: If confirmed, I will use the IC architecture and the IC CIO authorities to ensure the Community is implementing collaborative capabilities.

Recommendation 8: I understand work has been done in this area: A-Space is operational, and Intellipedia is a key knowledge sharing tool for the Community. If confirmed, I will further the implementation of collaborative capabilities.

Recommendation 9: Designing collaborative features into new workspaces from the ground up is important. Through oversight rather than by doing the implementation, the IC CIO will work with the appropriate IC elements to ensure that attention is given to the design of the collaborative IT environments and that the results actually foster collaboration.

Recommendation 11: If confirmed, I will support the IC-wide collaboration training effort by coordinating and focusing collaboration tool and computer-based learning expertise from across the IC.

43. Do you envision an IC enterprise with inclusion of our closest foreign allies as the rule and NOFORN as an exception, or vice versa? Would you offer another model for how well our foreign allies are integrated into our intelligence information systems?

I understand that minimizing the use of NOFORN is an ODNI priority. Policies such as Intelligence Community Directive (ICD) 208, Write for Maximum Utility and ICD 501 Information Sharing call for producing intelligence at the lowest classification level consistent with source protection, and producing tear-line versions of reports to support sharing with foreign partners. If confirmed, I will work with all ODNI elements to ensure that authorized users, foreign or otherwise, are able to receive information in an appropriate and timely manner.

44. In a March 23, 2009, letter to Director Blair, the Committee reiterated an interest in learning more about "which US information security standards apply to which IC information systems; the specific roles and responsibilities of the DNI for IC information security under relevant legislation, executive orders, and current practices; and the important roles and responsibilities for IC information security leadership that are not currently held by the DNI." Please provide your views on these topics.

This is a complex topic. There are numerous statutes and policies that provide relevant authorities to agency heads, and there are multiple governance bodies. Given this mix, there are overlaps, contradictions, different definitions/lexicons/taxonomies and questions about what applies to each system and agency. I understand the DNI and DoD have been working together to clarify these authority and governance issues. Clearly sorting this out must be a DNI priority.

45. Do you believe we should be developing data centers in the IC?

Yes. Shared data centers have the potential to reduce costs and support environmentally friendly objectives. If confirmed, I will review recent experience with data centers in industry and government, and use the information to evaluate options for the IC including planning,

building, and operating data centers that support the IC mission where the business case supports the approach.

46. Please comment on the merits or pitfalls of "virtualizing" portions of the enterprise architecture. What is your plan for "virtualizing" the various ground stations and data centers?

Virtualization is a viable approach to reducing cost and the IT footprint in many environments; however, the benefits of virtualization are situation-specific. If confirmed, I will review the IC environment and make informed decisions based on cost/benefit analysis.

47. If confirmed as the IC CIO, will you structure a service oriented architecture (SOA) governance model to support multiple requirements and future growth?

Yes. I believe a service-oriented environment is a good choice to support many of the IC's information requirements. As I learned in DoD, appropriate governance is essential to make required services available, to oversee service providers so that the services meet the needs and performance expectations of the users, to avoid unnecessary duplication and cost, and to prioritize new requirements.

48. What is your understanding of the IC CIO's obligation to make intelligence information available to remote areas, remote users, and/or bandwidth constrained users?

It is the IC CIO's responsibility to ensure through policy, architecture, and standards that IC users, including remote and/or bandwidth constrained users, can discover and retrieve the information they need, when they need it, and in a form that they can use to meet their mission needs. While the IC CIO does not implement or operate the capabilities that supply the information to the remote areas or bandwidth constrained users, the CIO establishes the architecture, standards, and requirements, and oversees the implementation by appropriate IC elements.

49. Duties and responsibilities of intelligence discipline functional managers have been defined in statute, executive orders, and departmental directives. Many of their responsibilities relate to establishing standards, IT protocols, and enterprise architecture decisions related to their intelligence disciplines. However, the signals intelligence and geospatial intelligence functional management authorities largely predate the creation of the DNI and Undersecretary of Defense for Intelligence (USD(I)). What enterprise architecture responsibilities, if any, that are currently considered the purview of the intelligence discipline functional managers do you believe should be transferred to a higher echelon (either the USD(I) or the DNI)? If none, how will you manage the overlapping authorities and responsibilities granted to both the IC CIO and the functional managers if you are confirmed?

The issue of legal authority for the establishment of standards, policies and guidelines for information technology in the IC is complex. If confirmed, I will work with the DNI to clarify, and look forward to the Committee's support.