Cyber Threat Intelligence Integration Center (CTIIC) 90-Day Status Report

On 25 February 2015, the President issued a memorandum to the Director of National Intelligence (DNI) directing that he establish a Cyber Threat Intelligence Integration Center (CTIIC) using his statutory authorities to create national intelligence centers. The memorandum calls on the DNI to provide a status report to the Director of the Office of Management and Budget and the Assistant to the President for Homeland Security and Counterterrorism within 90 days. This report further defines CTIIC's mission, roles, and responsibilities and outlines steps to be taken for CTIIC to reach initial operating capability by the beginning of fiscal year (FY) 2016.

1. Mission Responsibilities

The President assigned five responsibilities to CTIIC in the memorandum. The Office of the Director of National Intelligence (ODNI) conducted a comprehensive effort with assistance from senior intelligence officials from the Department of Homeland Security (DHS), Federal Bureau of Investigation (FBI), National Security Agency (NSA), Central Intelligence Agency (CIA), and Defense Intelligence Agency (DIA) to review current Intelligence Community (IC) cyber reporting and make recommendations as to how CTIIC should carry out these responsibilities given the staffing and resources requested for FY 2016. The Presidentially mandated functions are listed in bold text in A through E below, along with an explanation of the findings of the interagency team and identification of how CTIIC can carry out its assigned responsibilities:

A. **Provide integrated all-source analysis of intelligence related to foreign cyber threats or related to incidents affecting U.S. national interests.** The IC and its Federal partners generate a significant volume of information on foreign cyber threat actors, their capabilities, and their operational activity on a daily basis. This information ranges from individual intelligence reports on foreign cyber plans, capabilities, and operations to updates on investigations and actions taken in response to significant threats and incidents. However, these products are not uniform in focus and often describe different aspects of threat—or may describe the same aspect from the unique mission perspective of the reporting organization. These reports are published at differing intervals, often mask "actionable" information such as victim identification or impact for legitimate reasons, and may not reveal useful contextual information known to some part of government to a broader audience.

CTIIC will help to "connect the dots" by integrating and leveraging the insight and information already held by the Federal Government in order to produce a more timely and holistic understanding of foreign cyber threats. For current and near-term threats and for incidents, CTIIC can begin to achieve this by integrating existing government reports, summaries, and updates. CTIIC will normalize these often disparate perspectives using a common conceptual threat framework and lexicon and presenting reporting on the most salient or high priority threats in a fashion that provides context (the "so what" factor), as well as explicitly identifying gaps and limitations to our knowledge. CTIIC's current analysis and production will complement—not replace—existing department and agency cyber threat reports and analysis, which are generated to serve each organization's unique mission needs and customers. CTIIC's focus would be on creating a common baseline understanding of cyber threat and a frame of reference to improve shared situational awareness.

CTIIC will also integrate information on current and near-term foreign cyber threat capabilities and activities with the IC's expertise and intelligence on key adversaries' strategic decision-making and broader geopolitical factors. Nation-state cyber threat activity that has the potential to affect U.S. national and economic security is typically initiated or directed by a more senior foreign decision maker than the actual threat actor sitting behind the computer keyboard. Therefore, achieving a holistic understanding of when and how such threats will arise requires blending intelligence on near-term threat capabilities and current threat activities with the IC's more strategic insight into foreign decision making and the factors that might trigger the use of specific cyber capabilities.

CTIIC will leverage reporting and analysis already done across the U.S. Government (USG) to the greatest extent possible, focusing its production and in-house analysis on integration, filling time-sensitive gaps, and providing services of common concern as described in Section II of this report. Relevant information from other areas of government responsibility (e.g., investigation and incident response) will be integrated with threat intelligence to provide a unified perspective that helps policymakers more readily understand the magnitude of a particular threat or incident and helps them ensure that the appropriate actions are taken by government. Such integration can also give federal agencies information to enhance their cybersecurity posture and can provide those federal organizations chartered to do external cybersecurity—especially prevention, response, and mitigation—with more timely and actionable threat information to share with their private sector partners.

B. **Support the existing USG cyber centers and other USG organizations by ensuring that they have access to the necessary intelligence.** CTIIC will support the existing cyber centers and others by leading government activity to provide an integrated perspective on cyber threat as described above. In the process of generating its threat products, CTIIC can also identify gaps and improve the timeliness of collaboration by alerting agencies to prospective or logical follow up actions. Fulfilling the other functions assigned to CTIIC by the President and discussed elsewhere in this report—i.e., ensuring the downgrade and release of threat indicators, overseeing the development of intelligence sharing capabilities, and supporting interagency planning—will also allow CTIIC to improve the flow of intelligence to government organizations with cybersecurity, cyber intelligence, and policy missions. In these cases, CTIIC will serve in a supporting role, rather than as the lead center or as a consolidation of all government cybersecurity authorities and capabilities.

C. **Oversee the development and implementation of intelligence sharing capabilities (to include systems, programs, policies, and standards) to enhance shared situational awareness among USG organizations of foreign cyber threats to U.S. national interests.** Sharing information on a timely basis and in standardized form is vital for addressing the range of cyber threats to the networks that support our nation's public health and safety, national security, and economic security. CTIIC will provide strategic guidance and requirements to ongoing programs working to improve federal information sharing capabilities and for projects such as the automation of a common Cyber Threat Framework for use across the Federal Government.

D. **Ensure that indicators of malicious cyber activity and related threat intelligence reporting are downgraded for sharing with network defenders (USG and private sector) through existing processes.** Executive Order (EO) 13636, *Improving Critical Infrastructure Cybersecurity*, sets the imperative to increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities so that they may better protect and defend themselves against cyber threats. IC collectors are responsible for issuing sanitized versions (tearlines) of threat reporting; providing information for use in notifying identified targets or victims of foreign threat activity; and downgrading and releasing useful information to IC and other federal partners such as DHS, FBI, and sector-specific agencies to pass to the private sector, as appropriate, to meet the aims of EO 13636.

CTIIC itself will not engage or share intelligence directly with the private sector, nor will it be part of the downgrade or release process. However, like other recipients of intelligence reporting, it can request that a product be downgraded. CTIIC will also track the status of the IC's efforts to carry out its responsibility to downgrade cyber threat information, ensuring that systems used to request and pass such material generate metrics (e.g., numbers of reports downgraded, numbers passed by FBI or DHS to a victim) to measure performance and identify areas for improvement.

E. **Facilitate and support interagency efforts to develop and implement plans to counter foreign cyber threats using all instruments of national power.** CTIIC is uniquely positioned to look beyond individual department and agency missions toward an integrated effort to address the most significant malicious cyber actors. By supporting an integrated planning process, CTIIC can facilitate the synchronization of activities across multiple departments and agencies to execute whole-of-government cyber campaigns and with Federal partners to ensure that operational proposals contain measures of progress and success.

II. Core Functions

The ODNI review identified three core functions or lines of business the CTIIC should undertake to fulfill its assigned responsibilities and meet customer needs. The functions and the preliminary products and services the CTIIC will offer include:

A. **Watch Operations.** The CTIIC Watch will work collaboratively across cyber elements of the IC and other federal entities to develop and disseminate information to promote situational awareness and a common view of cyber threat intelligence and cyber events with potential impact on national security. To this end, the CTIIC watch will generate two products:

1. The Cyber Threat Intelligence Summary will be a daily product prepared in consultation with the IC that will summarize priority foreign cyber threats and identify actions the IC has taken in response, such as issuing tearline reporting that downgrades actionable intelligence and threat indictors to make them available for wider customer use. When possible, this summary will include additional material or commentary to provide context and improve understanding of the significance of these threats.

2. The Cyber Event Report will capture information regarding specific critical threats or incidents and document actions taken by the USG in response. The threshold for the generation of such reports will be based on the severity or potential impact of the event, regardless of whether it is deemed to be a foreign cyber threat. These reports will be produced under multi-seal authority integrating input on foreign threat activity from the IC with information on incident investigation and response activities. Non-IC content would be provided by the relevant departments and agencies, either directly or through their assignees housed in CTIIC, and operated under their home agency authorities. These Cyber Event Reports should also facilitate identification of information gaps and impediments to action and enable more efficient interagency coordination on emergent threats and incidents.

B. **Strategic Analysis.** The review also highlighted the value of more strategic analytic products, particularly for anticipatory products on threat actor intent. To date, the most significant cyber incidents have occurred in conjunction with geo-political tension and have been preceded by actions or statements that indicated intent. CTIIC's strategic analysis unit will be charged with working with USG communities of interest on the highest priority threat actors, serving as a catalyst to integrate the USG's understanding of their cyber capabilities and activities and identifying likely perpetrators and targets of malicious cyber activity based on all-source intelligence analysis. To both perform such indications and warning analysis and serve as a hub for providing integrated assessment of current activity and capability. CTIIC's small analytic staff will work closely and regularly with IC experts representing all of the disciplines related to cyber threat, especially technical, regional, and strategic analysis.

- Technical analysis will inform CTIIC regarding foreign threat actors' capabilities, and trends in operational behavior and tactics.
- Regional and leadership analysis (including foreign language media) will inform CTIIC regarding foreign threat actors' intentions and decision-making processes.
- Strategic analysis (including politico-economic, legal, diplomatic, international institutions, and global governance issues) will provide context, situational awareness, and, ideally, advance warning of events or conditions that might trigger the use of a cyber threat capability.

In addition to informing IC collection and USG cybersecurity efforts, these strategic products can also provide actionable "over the horizon" information that partners such as DHS and FBI can share with state, local, and tribal governments and with private sector partners.

C. **Support to Planning.** Operating under the policy direction of the President and the National Security Council, CTIIC can support strategic management of end-to-end processes needed for successful campaign development and execution in four ways.

1. CTIIC will provide strategic intelligence analysis prior to the initiation of campaign planning to describe the target's decision-making regarding use of cyber and its operational environment. This should provide a common baseline to help frame the "art of the possible" in terms of near-term campaign objectives. This is a lesson learned from the conduct of ongoing campaigns.

2. CTIIC will offer mechanisms such as meetings, a software portal, or other online collaborative tools through which draft initiatives, plans, and operational proposals can be more rapidly brought forward for interagency consideration and input. Doing this

early in the planning cycle should facilitate the identification of potential problems before significant resources have been invested by the originating organization, allow for more interactive interagency development of proposals, and lead to the generation of more timely and forward-leaning or actionable operational proposals by departments and agencies.

3. CTIIC and federal partners will work together to create a process and a framework through which identified lead agencies can provide standardized assessment of diplomatic, intelligence, military, economic, and other national equities potentially affected by any specific operational proposal. CTIIC itself would not perform these equity checks but would work with federal partners to ensure that designated lead agencies provide data and normalize it onto a common scale (e.g., low, medium, high) for policymakers' consideration.

4. CTIIC will work with departments and agencies to ensure that operational proposals contain measures of progress and success. CTIIC itself would not shape or define "mission success," but, when requested, could offer subject matter expertise on performance measurement.

The DNI recognizes the importance of ensuring that CTIIC's activities are conducted within the scope of ODNI's authorities and in a manner that complies with legal and policy requirements, which includes working with key stakeholders to identify and address potential legal, policy, and civil liberties issues. In addition, ODNI is also looking at building in appropriate mechanisms to ensure transparency, facilitate oversight, and enhance public understanding of CTIIC's activities.

III. Current Activities to Reach Initial Operating Capability

ODNI is taking a number of steps to plan for CTIIC to reach initial operating capability at the start of FY 2016. These include:

A. **Logistics and Location.** ODNI stood up a small team of officers to help plan for the establishment of CTIIC. This team is focused primarily on the programmatic aspects of the establishment of a new center—particularly on budget development; human capital needs and recruitment; information technology requirements and installation processes and timelines; and other facilities and equipment needs. Pending Congressional approval of CTIIC funding, the DNI plans to locate the new center at an existing ODNI facility in College Park, Maryland. All five functions described in this report will require additional information technology support as business processes are established and initial operations commence. We are currently identifying those requirements, as well as any out-year costs.

B. **Watch Product Pilots**. ODNI also plans to assemble a team to pilot the daily Watch prototype products described in this report. This team will comprise five assignees from IC elements and will be co-located with the National Counterterrorism Center's Operations Center in Liberty Crossing. Working as a notional CTIIC Watch day shift, the team will further refine the prototype products through practical experience and feedback from recipients. The Pilot Team will also develop business processes and test assumptions on the staffing and resources required to ensure adequate coverage based on the volume and tempo of incoming intelligence reporting and the demand for time-sensitive support from policymakers. This pilot effort will provide an opportunity to gauge the tempo, timing, and alternative mechanisms for dissemination of daily products, and will enable CTIIC to start from a set of tested processes and products as it reaches initial operating capability.

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu