PRESIDENTIAL POLICY DIRECTIVE/PPD-20

MEMORANDUM FOR THE VICE PRESIDENT
THE SECRETARY OF STATE
THE SECRETARY OF THE TREASURY
THE SECRETARY OF DEFENSE
THE ATTORNEY GENERAL
THE SECRETARY OF COMMERCE
THE SECRETARY OF ENERGY
THE SECRETARY OF HOMELAND SECURITY
ASSISTANT TO THE PRESIDENT AND CHIEF OF STAFF
DIRECTOR OF THE OFFICE OF MANAGEMENT AND BUDGET
ASSISTANT TO THE PRESIDENT FOR NATIONAL SECURITY AFFAIRS
DIRECTOR OF NATIONAL INTELLIGENCE
ASSISTANT TO THE PRESIDENT FOR HOMELAND SECURITY AND COUNTERTERRORISM
DIRECTOR OF THE OFFICE OF SCIENCE AND TECHNOLOGY POLICY
DIRECTOR OF THE FEDERAL BUREAU OF INVESTIGATION
DIRECTOR OF THE CENTRAL INTELLIGENCE AGENCY
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
DIRECTOR OF THE NATIONAL SECURITY AGENCY

SUBJECT: U.S. Cyber Operations Policy (U)

This Presidential Policy Directive (PPD) supersedes National Security Presidential Directive (NSPD)-38 of July 7, 2004. This directive complements, but does not affect, NSPD-54/Homeland Security Presidential Directive (HSPD)-23 on "Cybersecurity Policy" of January 8, 2008; National Security Directive (NSD)-42 on "National Policy for the Security of National Security Telecommunications and Information Systems" of July 5, 1990; and PPD-8 on "National Preparedness" of March 30, 2011. (C/NF)

I. Definitions (U)

The following terms are defined for the purposes of this directive and should be used when possible in interagency

documents and communications on this topic to ensure common understanding. (U)

Cyberspace: The interdependent network of information technology infrastructures that includes the Internet, telecommunications networks, computers, information or communications systems, networks, and embedded processors and controllers. (U)

Network Defense: Programs, activities, and the use of tools necessary to facilitate them (including those governed by NSPD-54/HSPD-23 and NSD-42) conducted on a computer, network, or information or communications system by the owner or with the consent of the owner and, as appropriate, the users for the primary purpose of protecting (1) that computer, network, or system; (2) data stored on, processed on, or transiting that computer, network, or system; or (3) physical and virtual infrastructure controlled by that computer, network, or system. Network defense does not involve or require accessing or conducting activities on computers, networks, or information or communications systems without authorization from the owners or exceeding access authorized by the owners. (U)

Malicious Cyber Activity: Activities, other than those authorized by or in accordance with U.S. law, that seek to compromise or impair the confidentiality, integrity, or availability of computers, information or communications systems, networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon. (U)

Cyber Effect: The manipulation, disruption, denial, degradation, or destruction of computers, information or communications systems, networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon. (U)

Cyber Collection: Operations and related programs or activities conducted by or on behalf of the United States Government, in or through cyberspace, for the primary purpose of collecting intelligence - including information that can be used for future operations - from computers, information or communications systems, or networks with the intent to remain undetected. Cyber collection entails accessing a computer, information system, or network without authorization from the owner or operator of that computer, information system, or network or from a party to a communication or by exceeding authorized access. Cyber collection includes those activities essential and inherent to enabling cyber collection, such as

inhibiting detection or attribution, even if they create cyber effects. (C/NF)

Defensive Cyber Effects Operations (DCEO): Operations and related programs or activities - other than network defense or cyber collection - conducted by or on behalf of the United States Government, in or through cyberspace, that are intended to enable or produce cyber effects outside United States Government networks for the purpose of defending or protecting against imminent threats or ongoing attacks or malicious cyber activity against U.S. national interests from inside or outside cyberspace. (C/NF)

Nonintrusive Defensive Countermeasures (NDCM): The subset of DCEO that does not require accessing computers, information or communications systems, or networks without authorization from the owners or operators of the targeted computers, information or communications systems, or networks or exceeding authorized access and only creates the minimum cyber effects needed to mitigate the threat activity. (C/NF)

Offensive Cyber Effects Operations (OCEO): Operations and related programs or activities - other than network defense, cyber collection, or DCEO - conducted by or on behalf of the United States Government, in or through cyberspace, that are intended to enable or produce cyber effects outside United States Government networks. (C/NF)

Cyber Operations: Cyber collection, DCEO (including NDCM), and OCEO collectively. (U)

Significant Consequences: Loss of life, significant responsive actions against the United States, significant damage to property, serious adverse U.S. foreign policy consequences, or serious economic impact on the United States. (U)

U.S. National Interests: Matters of vital interest to the United States to include national security, public safety, national economic security, the safe and reliable functioning of "critical infrastructure," and the availability of "key resources."[1] (U)

Emergency Cyber Action: A cyber operation undertaken at the direction of the head of a department or agency with appropriate authorities who has determined that such action is necessary, pursuant to the requirements of this directive, to mitigate an imminent threat or ongoing attack against U.S. national interests from inside or outside cyberspace and under circumstances that at the time do not permit obtaining prior

[1] As these terms are used in HSPD-7 on "Critical Infrastructure, Identification, Prioritization, and Protection" from December 17, 2003. (U)

Presidential approval to the extent that such approval would otherwise be required. (S/NF)

II. Purpose and Scope (U)

The United States has an abiding interest in developing and maintaining use of cyberspace as an integral part of U.S. national capabilities to collect intelligence and to deter, deny, or defeat any adversary that seeks to harm U.S. national interests in peace, crisis, or war. Given the evolution in U.S. experience, policy, capabilities, and understanding of the cyber threat, and in information and communications technology, this directive establishes updated principles and processes as part of an overarching national cyber policy framework. (C/NF)

The United States Government shall conduct all cyber operations consistent with the U.S. Constitution and other applicable laws and policies of the United States, including Presidential orders and directives. (C/NF)

The United States Government shall conduct DCEO and OCEO under this directive consistent with its obligations under international law, including with regard to matters of sovereignty and neutrality, and, as applicable, the law of armed conflict. (C/NF)

This directive pertains to cyber operations, including those that support or enable kinetic, information, or other types of operations. Most of this directive is directed exclusively to DCEO and OCEO. (S/NF)

The United States Government has mature capabilities and effective processes for cyber collection. (S/NF)

Therefore, this directive affirms and does not intend to alter existing procedures, guidelines, or authorities for cyber collection. (S/NF)

This directive provides a procedure for cyber collection operations that are reasonably likely to result in "significant consequences."[2] (S/NF)

The principles and requirements in this directive apply except as otherwise lawfully directed by the President. With the exception of the grant of authority to the Secretary of Defense to conduct Emergency Cyber Actions as provided below, nothing in this directive is intended to alter the existing authorities of, or grant new authorities to, any United States Government department or agency (including authorities to carry out

[2] NSPD-38 referred to operations with significant consequences as "sensitive offensive cyber operations." (S/NF)

operational activities), or supersede any existing coordination and approval processes, other than those of NSPD-38. Nothing in this directive is intended to limit or impair military commanders from using DCEO or OCEO specified in a military action approved by the President and previously coordinated and deconflicted as required by existing processes and this directive. (S/NF)

In addition, this directive does not pertain to or alter existing authorities related to the following categories of activities by or on behalf of the United States Government, regardless of whether they produce cyber effects:

- Activities conducted under section 503 of the National Security Act of 1947 (as amended);
- Activities conducted pursuant to the Foreign Intelligence Surveillance Act, the approval authority delegated to the Attorney General (AG) by section 2.5 of Executive Order 12333 (as amended), or law enforcement authorities; however, cyber operations reasonably likely to result in significant consequences still require Presidential approval, and operations that reasonably can be expected to adversely affect other United States Government operations still require coordination under established processes;
- Activities conducted by the United States Secret Service for the purpose of protecting the President, the Vice President, and others as defined in 18 U.S.C. § 3056; however, cyber operations reasonably likely to result in significant consequences still require Presidential approval, and operations that reasonably can be expected to adversely affect other United States Government operations still require coordination under established processes;
- The use of online personas and other virtual operations[3] - undertaken exclusively for counterintelligence, intelligence collection, or law enforcement purposes - that do not involve the use of DCEO or OCEO;
- Activities conducted in cyberspace pursuant to counterintelligence authorities for the purpose of protecting specific intelligence sources, methods, and activities;
- Signals intelligence collection other than cyber collection as defined in this directive;
- Open-source intelligence collection;
- Network defense;

[3] Human intelligence operations undertaken via the Internet. (S/NF)

Traditional electronic warfare[4] activities;

The development of content to support influence campaigns, military deception, or military information support operations; or

Simple transit of data or commands through networks that do not create cyber effects on those networks. (S/NF)

III. Guiding Principles for DCEO and OCEO (U)

DCEO and OCEO may raise unique national security and foreign policy concerns that require additional coordination and policy considerations because cyberspace is globally connected. DCEO and OCEO, even for subtle or clandestine operations, may generate cyber effects in locations other than the intended target, with potential unintended or collateral consequences that may affect U.S. national interests in many locations. (S/NF)

The United States Government shall conduct DCEO and OCEO in a manner consistent with applicable values, principles, and norms for state behavior that the United States Government promotes domestically and internationally as described in the 2011 "International Strategy for Cyberspace." (C/NF)

National-level strategic objectives and operational necessities shall dictate what the United States Government seeks to accomplish with DCEO and OCEO. (C/NF)

The United States Government shall integrate DCEO and OCEO, as appropriate, with other diplomatic, informational, military, economic, financial, intelligence, counterintelligence, and law enforcement options, taking into account effectiveness, costs, risks, potential consequences, foreign policy, and other policy considerations. (C/NF)

The United States Government shall reserve the right to act in accordance with the United States' inherent right of self defense as recognized in international law, including through the conduct of DCEO. (C/NF)

The United States Government shall conduct neither DCEO nor OCEO that are intended or likely to produce cyber effects within the United States unless approved by the President. A department or agency, however, with appropriate authority may

[4] As defined by the Joint Dictionary 1-02, "Department of Defense Dictionary of Military and Associated Terms" (as amended through February 15, 2012): military action involving the use of electromagnetic or directed energy to control the electromagnetic spectrum or to attack the enemy. Electronic warfare consists of three divisions: electronic attack, electronic protection, and electronic warfare support. (U)

conduct a particular case of DCEO that is intended or likely to produce cyber effects within the United States if it qualifies as an Emergency Cyber Action as set forth in this directive and otherwise complies with applicable laws and policies, including Presidential orders and directives. (C/NF)

The United States Government shall obtain consent from countries in which cyber effects are expected to occur or those countries hosting U.S. computers and systems used to conduct DCEO or OCEO unless:

Military actions approved by the President and ordered by the Secretary of Defense authorize nonconsensual DCEO or OCEO, with provisions made for using existing processes to conduct appropriate interagency coordination on targets, geographic areas, levels of effect, and degrees of risk for the operations;

DCEO is undertaken in accordance with the United States' inherent right of self defense as recognized in international law, and the United States Government provides notification afterwards in a manner consistent with the protection of U.S. military and intelligence capabilities and foreign policy considerations and in accordance with applicable law; or

The President - on the recommendation of the Deputies Committee and, as appropriate, the Principals Committee - determines that an exception to obtaining consent is necessary, takes into account overall U.S. national interests and equities, and meets a high threshold of need and effective outcomes relative to the risks created by such an exception. (S/NF)

The information revealed to other countries in the course of seeking consent shall be consistent with operational security requirements and the protection of intelligence sources, methods, and activities. (S/NF)

The United States Government, to ensure appropriate application of these principles, shall make all reasonable efforts, under circumstances prevailing at the time, to identify the adversary and the ownership and geographic location of the targets and related infrastructure where DCEO or OCEO will be conducted or cyber effects are expected to occur, and to identify the people and entities, including U.S. persons, that could be affected by proposed DCEO or OCEO. (S/NF)

Additional Considerations for DCEO (U)

The Nation requires flexible and agile capabilities that leverage the full resources of the United States Government to conduct necessary and proportionate DCEO. These operations shall conform to the following additional policy principles:

The United States Government shall reserve use of DCEO to protect U.S. national interests in circumstances when network defense or law enforcement measures are insufficient or cannot be put in place in time to mitigate a threat, and when other previously approved measures would not be more appropriate, or if a Deputies or Principals Committee review determines that proposed DCEO provides an advantageous degree of effectiveness, timeliness, or efficiency compared to other methods commensurate with the risks;

The United States Government shall conduct DCEO with the least intrusive methods feasible to mitigate a threat;

The United States Government shall seek partnerships with industry, other levels of government as appropriate, and other nations and organizations to promote cooperative defensive capabilities, including, as appropriate, through the use of DCEO as governed by the provisions in this directive; and

Partnerships with industry and other levels of government for the protection of critical infrastructure shall be coordinated with the Department of Homeland Security (DHS), working with relevant sector-specific agencies and, as appropriate, the Department of Commerce (DOC). (S/NF)

The United States recognizes that network defense, design, and management cannot mitigate all possible malicious cyber activity and reserves the right, consistent with applicable law, to protect itself from malicious cyber activity that threatens U.S. national interests. (S/NF)

The United States Government shall work with private industry - through DHS, DOC, and relevant sector-specific agencies - to protect critical infrastructure in a manner that minimizes the need for DCEO against malicious cyber activity; however, the United States Government shall retain DCEO, including anticipatory action taken against imminent threats, as governed by the provisions in this directive, as an option to protect such infrastructure. (S/NF)

The United States Government shall - in coordination, as appropriate, with DHS, law enforcement, and other relevant departments and agencies, to include sector-specific agencies - obtain the consent of network or computer owners for United States Government use of DCEO to protect against malicious cyber activity on their behalf, unless the activity

implicates the United States' inherent right of self-defense as recognized in international law or the policy review processes established in this directive and appropriate legal reviews determine that such consent is not required. (S/NF)

Offensive Cyber Effects Operations (U)

OCEO can offer unique and unconventional capabilities to advance U.S. national objectives around the world with little or no warning to the adversary or target and with potential effects ranging from subtle to severely damaging. The development and sustainment of OCEO capabilities, however, may require considerable time and effort if access and tools for a specific target do not already exist. (TS/NF)

The United States Government shall identify potential targets of national importance where OCEO can offer a favorable balance of effectiveness and risk as compared with other instruments of national power, establish and maintain OCEO capabilities integrated as appropriate with other U.S. offensive capabilities, and execute those capabilities in a manner consistent with the provisions of this directive. (TS/NF)

IV. Cyber Operations with Significant Consequences (U)

Specific Presidential approval is required for any cyber operations - including cyber collection, DCEO, and OCEO - determined by the head of a department or agency to conduct the operation to be reasonably likely to result in "significant consequences" as defined in this directive. This requirement applies to cyber operations generally, except for those already approved by the President, even if this directive otherwise does not pertain to such operations as provided in the "Purpose and Scope" section of this directive. (S/NF)

V. Threat Response Operations (U)

Responses to Persistent Malicious Cyber Activity (U)

Departments and agencies with appropriate authorities - consistent with the provisions set forth in this directive and in coordination with the Departments of State, Defense (DOD), Justice (DOJ), and Homeland Security; the Federal Bureau of Investigation (FBI); the Office of the Director of National Intelligence (DNI); the National Security Agency (NSA); the Central Intelligence Agency (CIA); the Departments of the Treasury and Energy (DOE); and other relevant members of the Intelligence Community (IC) and sector-specific agencies - shall establish criteria and procedures to be approved by the

President for responding to persistent malicious cyber activity against U.S. national interests. Such criteria and procedures shall include the following requirements:

The United States Government shall reserve use of such responses to circumstances when network defense or law enforcement measures are insufficient or cannot be put in place in time to mitigate the malicious cyber activity; and

Departments and agencies shall conduct these responses in a manner not reasonably likely to result in significant consequences and use the minimum action required to mitigate the activity. (S/NF)

Emergency Cyber Actions (C/NF)

The Secretary of Defense is hereby authorized to conduct, or a department or agency head with appropriate authorities may conduct, under procedures approved by the President, Emergency Cyber Actions necessary to mitigate an imminent threat or ongoing attack using DCEO if circumstances at the time do not permit obtaining prior Presidential approval (to the extent that such approval would otherwise be required) and the department or agency head determines that:

An emergency action is necessary in accordance with the United States inherent right of self-defense as recognized in international law to prevent imminent loss of life or significant damage with enduring national impact on the Primary Mission Essential Functions of the United States Government,[5] U.S. critical infrastructure and key resources, or the mission of U.S. military forces;

Network defense or law enforcement would be insufficient or unavailable in the necessary timeframe, and other previously approved activities would not be more appropriate;

The Emergency Cyber Actions are reasonably likely not to result in significant consequences;

The Emergency Cyber Actions will be conducted in a manner intended to be nonlethal in purpose, action, and consequence;

The Emergency Cyber Actions will be limited in magnitude, scope, and duration to that level of activity necessary to mitigate the threat or attack;

The Emergency Cyber Actions, when practicable, have been coordinated with appropriate departments and agencies, including State, DOD, DHS, DOJ, the Office of the DNI, FBI, CIA, NSA, the Treasury, DOE, and other relevant members of the IC and sector-specific agencies; and

[5] As defined in NSPD-51/HSPD-20 on "National Continuity Policy" of May 9, 2007. (U)

The Emergency Cyber Actions are consistent with the U.S. Constitution and other applicable laws and policies of the United States, including Presidential orders and directives. (S/NF)

In addition, Emergency Cyber Actions that are intended or likely to produce cyber effects within the United States (or otherwise likely to adversely affect U.S. network defense activities or U.S. networks) must be conducted:

Under the procedures and, as appropriate, criteria for domestic operations previously approved by the President; and

Under circumstances that at the time of the Emergency Cyber Action preclude the use of network defense, law enforcement, or some form of DOD support to civil authorities that would prevent the threatened imminent loss of life or significant damage. (S/NF)

Department and agency heads shall report Emergency Cyber Actions to the President through the National Security Advisor as soon as feasible. If the coordination specified above is not practicable in the available time, then notification shall occur after the fact as soon as possible to inform subsequent whole-of-government response and recovery activities. (S/NF)

Until such time as any additional criteria for domestic operations are approved by the President, authorization by department and agency heads for Emergency Cyber Actions that are intended or likely to produce cyber effects within the United States (or otherwise likely to adversely affect U.S. network defense activities or U.S. networks) shall be granted only if the President has provided prior approval for such activity, or circumstances at the time do not permit obtaining prior approval from the President and such actions are conducted within the other constraints defined above. (S/NF)

VI. Process (U)

The National Security Staff (NSS) shall formalize the functions of the Cyber Operations Policy Working Group (COP-WG) as the primary United States Government forum below the level of an Interagency Policy Committee (IPC) for integrating DCEO or OCEO policy, including consideration of exceptions or refinements to the principles of this directive. The COP-WG shall work with other elements of the policy community as appropriate to the geographic or functional context of the DCEO- or OCEO-related policy discussion at the earliest opportunity. The COP-WG is

not an operational group, but will address policy issues related to the conduct of operations raised by departments and agencies or the NSS. (S/NF)

Departments and agencies shall work through the COP-WG to raise unresolved or ambiguous policy questions in an integrated IPC meeting of all appropriate national and economic security stakeholders. The NSS shall use existing channels to elevate any unresolved policy conflicts to the Deputies and Principals Committees, as appropriate. (C/NF)

Departments and agencies shall continue to use existing operational processes for cyber operations, except as those processes are modified by or under this directive. Other types of operations that are supported or enabled by cyber operations shall use their existing operational processes. This continued use of existing operational processes applies, for example, to operations conducted under military orders that authorize DCEO or OCEO, including clandestine preparatory activities. (C/NF)

Departments and agencies, during planning for proposed cyber operations, shall use established processes[6] to coordinate and deconflict with other organizations - including, as appropriate, State, DOD, DOJ, DHS, members of the IC, and relevant sector-specific agencies - and obtain any other approvals required under applicable policies, except as those processes are modified by or under this directive. Departments and agencies shall modify or enhance these processes as future circumstances dictate. (S/NF)

Departments and agencies shall coordinate DCEO and OCEO with State and Chiefs of Station or their designees in countries where DCEO or OCEO are conducted or cyber effects are expected to occur. (S/NF)

Coordination of DCEO and OCEO with network defense efforts shall be sufficient to enable a whole-of-government approach to the protection of U.S. national interests and shall identify potential implications of proposed DCEO and OCEO for U.S. networks, including potential adversary responses or unintended consequences of U.S. operations for which the United States Government or the private sector would need to prepare. This coordination shall occur in a manner consistent with operational

[6] Including the May 9, 2007, "Trilateral Memorandum of Agreement (MOA) among the Department of Defense and the Department of Justice and the Intelligence Community Regarding Computer Network Attack and Computer Network Exploitation Activities," and other operational coordination processes that exist between departments and agencies. (S/NF)

security requirements and the protection of intelligence sources, methods, and activities. (S/NF)

Toward this end of ensuring a unified whole-of-government approach, departments and agencies shall coordinate and deconflict DCEO and OCEO with network defense efforts of other departments and agencies as appropriate. (S/NF)

In addition, DCEO and OCEO with potential implications for U.S. networks shall be deconflicted as appropriate and coordinated with DHS, appropriate law enforcement agencies, and relevant sector-specific agencies. (S/NF)

The United States Government shall make all reasonable efforts to identify and notify, as appropriate, private sector entities that could be affected by DCEO and OCEO. (S/NF)

Policy Criteria (U)

Policy deliberations for DCEO and OCEO shall consider, but not be limited to, the following criteria:

Impact: The potential threat from adversary actions or the potential benefits, scope, and recommended prioritization of proposed U.S. operations as compared with other approaches - including, as appropriate, network defense by the United States Government or private sector network operators;

Risks: Assessments of intelligence gain or loss, the risk of retaliation or other impacts on U.S. networks or interests (including economic), impact on the security and stability of the Internet, and political gain or loss to include impact on foreign policies, bilateral and multilateral relationships (including Internet governance), and the establishment of unwelcome norms of international behavior;

Methods: The intrusiveness, timeliness, efficiency, capacity, and effectiveness of operational methods to be employed;

Geography and Identity: Geographic and identity aspects of the proposed activity, including the location of operations and the resulting effects, the identity of network owners and users that will be affected, and the identity or type - when known - of adversaries to be countered or affected by U.S. operations;

Transparency: The need for consent or notification of network or computer owners or host countries, the potential for impact on U.S. persons and U.S. private sector networks, and the need for any public or private communications strategies before or after an operation; and

Authorities and Civil Liberties: The available authorities and procedures and the potential for cyber effects inside the United States or against U.S. persons. (S/NF)

Policy decisions shall be broad enough and include rationales in order to provide guidelines and direction for future proposals with the same operational and risk parameters. (C/NF)

Annex: Implementation (U)

Departments and agencies shall establish necessary capabilities and procedures for appropriate and timely implementation of DCEO and OCEO policies in the national interest. (C/NF)

Policy Process (U)

Departments and agencies shall, as appropriate, conduct DCEO and OCEO in accordance with the principles set forth in this directive and shall bring forward to the COP-WG situations that require policy discussion, including considerations of exceptions to those principles, using the policy criteria described in this directive. **[Action: All; ongoing]** (C/NF)

The National Security Advisor, through the NSS, shall establish and operate the COP-WG to serve as the entry point for interagency deliberations of policy matters related to DCEO and OCEO. **[Action: NSS; ongoing]** (C/NF)

The National Security Advisor, through the NSS, as needed, shall use the existing policy escalation process through an appropriate joint IPC-level group involving all stakeholders for a given situation, the Deputies Committee, and the Principals Committee. This process shall clarify the application of the principles set forth in this directive to specific operations, including consideration of exceptions or refinements to those principles. **[Action: NSS; ongoing]** (C/NF)

The NSS, as needed, shall lead reviews by appropriate departments and agencies of legal issues associated with DCEO and OCEO. The NSS shall refer legal questions to the chief legal officers of the appropriate departments or agencies or to DOJ for resolution of interagency disagreements or as otherwise appropriate. **[Action: NSS; ongoing]** (C/NF)

The DNI shall continue to ensure, through appropriate policies and procedures, the deconfliction, coordination, and integration of all IC cyber operations and serve as the IC focal point for strategic planning and policy coordination related to cyber operations, both within the IC and with other departments and agencies in interagency coordination processes. **[Action: DNI; ongoing]** (C/NF)

Policy Reviews and Preparation (U)

The Office of the DNI, in coordination with appropriate departments and agencies, shall prepare a classification guide for departments and agencies to use in the implementation of the policies in this directive. **[Action: Office of the DNI; 2 months after directive approval]** (U)

The National Security Advisor, through the NSS, shall lead an interagency review of the United States Government's communications strategy, including public affairs guidance, regarding DCEO and OCEO. Pending approval of this strategy by the Deputies Committee, the United States Government's public posture on related matters shall be: "All United States Government activities in cyberspace are consistent with the principles stated in the May 2011 *International Strategy for Cyberspace.*" **[Action: NSS report to Deputies; 1 month after directive approval]** (C/NF)

The National Security Advisor, through the NSS, shall work with the Secretaries of Defense, State, and Homeland Security, the AG, the DNI, relevant IC and sector-specific agencies, and other heads of departments and agencies as appropriate to develop for the conduct of Emergency Cyber Actions, as set forth in this directive - in addition to the previously cited procedures and, as appropriate, domestic criteria to be approved by the President - detailed concepts of operation, supporting processes, communications capabilities, exercises, and training. In addition, the NSS - working with these same departments and agencies - shall, as necessary, develop for Presidential approval procedures and criteria for DCEO to be conducted in response to malicious cyber activity. **[Action: NSS update on implementation to Deputies; 3 months after directive approval]** (C/NF)

The Secretary of Defense, the DNI, and the Director of the CIA - in coordination with the AG, the Secretaries of State and Homeland Security, and relevant IC and sector-specific agencies - shall prepare for approval by the President through the National Security Advisor a plan that identifies potential systems, processes, and infrastructure against which the United States should establish and maintain OCEO capabilities; proposes circumstances under which OCEO might be used; and proposes necessary resources and steps that would be needed for implementation, review, and updates as U.S. national security needs change. **[Action: DOD, Office of the DNI, and CIA update to Deputies on scope of plans; 6 months after directive approval]** (TS/NF)

The Secretary of Defense and other department and agency heads as appropriate - in coordination with the Secretary of Homeland Security, the AG, and the DNI - shall develop and maintain a flexible, agile capability for the purpose of using DCEO to defend U.S. networks consistent with the provisions set forth in this directive. **[Action: DOD and others; ongoing]** (C/NF)

The Secretary of Defense - in coordination with the Secretaries of Homeland Security, Commerce, and State, the AG, the DNI, and relevant IC and sector-specific agencies - shall develop a multi-phase plan to be approved by the Deputies Committee for testing, reviewing, and implementing NDCM. The plan shall be subjected to legal review and address authorities, technical feasibility, operational risks, and coordination procedures. **[Action: DOD present first phase of plans to Deputies; 2 months after directive approval]** (S/NF)

The AG and the DNI - in collaboration with the Secretaries of Defense, State, Commerce, and Homeland Security, and relevant IC and sector-specific agencies - shall develop a multi-phase plan to be approved by the Deputies Committee for a test of the applicability and efficacy of counterintelligence authorities in the conduct of DCEO. The plan shall be subjected to legal review and address technical feasibility, operational risks, and coordination procedures. **[Action: DOJ and Office of the DNI present first phase of plans to Deputies; 2 months after directive approval]** (S/NF)

The Secretaries of Defense and Homeland Security, the DNI, the AG, and the Director of the CIA - in collaboration as appropriate with the Secretaries of State and Commerce and the heads of relevant IC and sector-specific agencies - shall develop proposals to be approved by the President through the National Security Advisor to ensure that a necessary framework of proposed options, roles, and levels of delegation is in place for the use of all appropriate United States Government DCEO and OCEO capabilities to advance and defend U.S. national interests, including actions taken in response to indications of imminent threat or when the United States or the Internet is subjected to a debilitating attack. This framework shall consider how cyber operations capabilities will complement other United States Government cyber capabilities, including network defense and law enforcement. **[Action: DOD, DHS, DOJ, Office of the DNI, and CIA update to Deputies; 6 months after directive approval]** (S/NF)

Department and agency heads conducting DCEO or OCEO covered under this directive shall report annually on the use and effectiveness of operations of the previous year to the

President through the National Security Advisor. **[Action: relevant departments and agencies; ongoing until otherwise directed]** (S/NF)

Foundation Building (U)

The DNI, working with appropriate departments and agencies, shall continue to lead interagency efforts to improve intelligence collection in support of DCEO and OCEO, including under conditions when Internet infrastructure is significantly degraded. These efforts shall include an enhanced process for sharing intelligence-based cyber threat information with the private sector and international partners in the interest of minimizing the need for DCEO. The DNI shall identify needed investments - including in research and development, testing, and evaluation - to help develop intelligence capabilities in support of DCEO and OCEO. **[Action: Office of the DNI; ongoing]** (S/NF)

The Secretary of State - in coordination with the Secretaries of Defense and Homeland Security, the AG, the DNI, and others as appropriate - shall continue to lead efforts to establish an international consensus around norms of behavior in cyberspace to reduce the likelihood of and deter actions by other nations that would require the United States Government to resort to DCEO. **[Action: State; ongoing]** (C/NF)

The AG - through the FBI and in coordination as appropriate with DHS, appropriate elements of the IC, and other departments and agencies - shall continue to identify, investigate, mitigate, and disrupt malicious cyber activity in the interest of minimizing the need for DCEO. The AG, through the National Cyber Investigative Joint Task Force, shall lead related interagency efforts by integrating, sharing, coordinating, and collaborating on counterintelligence, counterterrorism, intelligence, and law enforcement information from member organizations concerning investigations of malicious cyber activity in order to facilitate the use of all available authorities to address such threats. These activities shall be coordinated with other entities and the private sector as appropriate. **[Action: DOJ; ongoing]** (C/NF)

The Secretaries of State, Defense, Homeland Security, and Commerce - along with the AG, the DNI, and others as appropriate - shall continue to advance interagency efforts with international partners to increase their cyber capacities for self protection and, where appropriate, to facilitate cooperative defense of cyberspace in the interest of minimizing the need for DCEO. The partnerships shall include

application of not only improvements to network defenses, but also sharing - as appropriate and consistent with operational security requirements and the protection of intelligence sources, methods, and activities - of DCEO-related information, tools, and methods consistent with the provisions set forth in this directive, the National Disclosure Policy, and with U.S. national interests. **[Action: State, DOD, DHS, DOC, and Office of the DNI; ongoing]** (C/NF)

The Secretary of Homeland Security - in coordination with the Secretaries of Defense and Commerce, the AG, the DNI, and the heads of relevant sector-specific agencies - shall continue to lead interagency efforts to develop partnerships with other levels of government and the private sector to increase the nation's cyber capacities for self protection and, where appropriate, to facilitate cooperative efforts to secure cyberspace in the interest of minimizing the need for DCEO. **[Action: DHS; ongoing]** (C/NF)