Appendix A – National OPSEC Program Requirements and Minimum Standards

(U) Signed 13 January 2021

(U) Identified Executive Branch tasks noted in NSPM-28

Table listing Executive Branch NSPM-28 items				
	Entity	**Task**	**Timeframe specified (if any)**	**Page identified**
Agency responsibilities (below)				
1.	Agencies	Shall employ the NOP to inform OPSEC and data management policies and procedures and to effect unified Federal engagement to counter threats as they emerge.		Page 6
2.	Agencies	May protect unclassified OPSEC Critical Information as CUI under EO 13556 of 4 November 2010, Controlled Unclassified Information, as a supplemental mitigation measure where appropriate.		Page 7
3.	Agencies	Shall, where appropriate, partner with State, local, tribal, and territorial government entities and the private sector to inform and support the integration of the NOP into their operations and activities.		Page 7
4.	Agencies	Should, as necessary and where appropriate, include partnering with the IC, law enforcement agencies, and other agencies to strengthen awareness of threats from foreign intelligence operations and other adversaries. Such support shall include raising risk awareness, identifying Critical Information and indicators that may be of use to an adversary, providing analysis of risks associated with the information, recommending or implementing appropriate countermeasures (including measures intended to reduce or eliminate impediments to effective cooperation), and when possible, preventing unnecessary duplication of effort.		Page 7
5.	Agencies	Shall inform NOP Office staff of such engagements and support [with/of IC, law enforcement agencies, State, local, tribal, territorial government entities] to improve		Page 7

		coordination, avoid conflict, and facilitate efficient use of resources.		
6.	Agencies	Shall, in accordance with NSPM-28, establish organizational OPSEC programs commensurate with the scope of their mission and responsibilities.		Page 7
7.	Agencies	Shall fund and maintain organizational OPSEC programs consistent with the level of risk presented to the agency's mission and activities to promote accountability for critical assets.		Page 7
8.	Agencies	Shall promulgate guidance, as needed, to reflect OPSEC resources, unique mission and training requirement, and organizational OPSEC objectives		Page 8
9.	Agencies	Shall coordinate and facilitate OPSEC assessments by the NOP Office staff.		Page 8
10.	Agencies	Shall provide NOP Office staff appropriate access, information, and support as necessary to facilitate the NOP Office mission when engaging with the agency.		Page 9
11.	Agencies	Shall share, if desired, unclassified and classified OPSEC threat information and mitigation guidance concerning US interests with State, local, tribal and territorial government entities, and the private sector, to address OPSEC threats to their operations and activities, in accordance with established authorities.		Page 9
12.	Agencies	May share classified information only in accordance with EO 13526 or any successor order.		Page 9
13.	Agencies	Will only share CUI in accordance with EO 13556.		Page 9
14.	Agencies	Shall implement NOP Office conclusions and recommendations resulting from NOP assessments, as described more fully in Section 6(f) of NSPM 28. An agency may challenge, in writing, a conclusion or recommendation by providing the challenge to NCSC within 60 days of receipt. Where no agreement can be reached, and notwithstanding the agency's own obligation under Section 4(b) of NSPM-28, the agency shall raise the issue to the National OPSEC Program Policy Coordination Committee (NOP PCC).		Page 9 and page 12

		Potential challenges include areas where there is disagreement on the risk associated with a threat, the effectiveness of recommended mitigations, or the agency's ability to implement recommendations.		
15.	Agencies	Shall establish cooperation between the agency's OPSEC program and its continuity of operations elements to ensure effective coordination of the agency's mission essential functions and agency's Critical Information.		Page 9
16.	Agencies	Are responsible for implementing NOP Offices conclusions and recommendations, but may challenge these conclusions and recommendations.		Page 12
17.	Agencies (including their contractors, sub-contractors, licensees, and grantees)	Shall incorporate the OPSEC Cycle into the planning, execution, and assessment of their operations, processes, and activities.		Page 6
18.	Agencies and agency heads	Shall establish an organizational OPSEC program commensurate with the agency's organizational mission, responsibilities, and risks, if the agency does not already have a program.	Within 360 days of the effective date of NSPM-28	Page 8
19.	Agencies and agency heads	Shall designate a senior official or officials with authority to provide management, accountability, and oversight of the agency's OPSEC program.	Within 360 days of the effective date of NSPM-28	Page 8
20.	Agencies and agency heads	Shall designate agency representatives to coordinate with the NOP Office as appropriate to support OPSEC activities, with specific qualifications and categories of assignment for each representative.	Within 360 days of the effective date of NSPM-28	Page 8
21.	Agencies and agency heads	Shall perform a self-assessment of the agency's OPSEC Posture and provide results of this assessment for NOP Office staff review. The results or related information from the self-assessment will be the property of the originating agency, and the NOP Office staff shall not disseminate the results without the express permission of originating agency.	Within 360 days of the effective date of NSPM-28	Page 8

22.	Agencies and agency heads	Shall develop and implement information-sharing policies and procedures, consistent with existing policies and procedures, to ensure NOP-relevant information, risks, or mitigation strategies are shared with the NCSC and other authorized partners.	Within 360 days of the effective date of NSPM-28	Page 8
23.	Agencies with access to classified information and insight into OPSEC threats	Shall support other agencies without such access by identifying Critical Information that may be of use to an adversary, providing analysis of risks associated with external threats to Critical Information, recommending or implementing appropriate countermeasures, and other appropriate information sharing.		Page 6
24.	Agency OPSEC assessments	Shall be conducted at the request of the agency head, the National OPSEC Program Policy Coordination Committee (NOP PCC), or by the head of the NOP Office with the concurrence of the agency head or designee and a minimum of 30 days prior notice, or sooner when time-sensitive NOP-related issues of significant concern exist or are reasonably suspected.		Page 8
OPSEC responsibilities (below)				
1.	OPSEC capabilities	Shall include Identity Management principles, including the protection of personally identifiable information (PII), which is a type of CUI.		Page 6
2.	OPSEC capabilities	Must include the ability to assess digital systems and databases for information or OPSEC indicators that adversaries and competitors can use to identify Critical Information.		Page 6
3.	Organizational OPSEC programs	Shall be integrated with counterintelligence and other security programs, such as those used to address insider threats, CUI, data loss prevention, cybersecurity, Foreign Access Management, physical security, industrial security, and information security.		Page 7
Other entities mentioned				
	National Archives and Records Administration	Shall develop a new category of CUI to be designated CUI OPSEC Critical Information, pursuant to EO 13556 of 4 November 2010, Controlled Unclassified Information.		Page 7

	Secretary of Energy	Shall retain authority over the distribution of Restricted Data and Formerly Restricted Data under the Atomic Energy Act of 1954, as amended, and regulations issued under that Act.		Page 9
	NSA's former Interagency OPSEC Support Staff (IOSS)	Shall incorporate its activities and resources into the NOP Office to ensure unity of effort and resource efficiency while preserving, to the extent possible, existing OPSEC training expertise.		Page 6
	NSC staff	Shall establish a National OPSEC Program Policy Coordination Committee (NOP PCC).		Page 9