Executive Order xxxxx of Month and Day 2025
Coordinating National Resilience to Adversarial Surveillance, Reconnaissance, and Weaponized Unmanned Aerial Systems
By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. ***Purpose.***
Adversarial Unmanned Aerial Systems (UAS) have the potential to disrupt, degrade, and damage technology and critical infrastructure systems. Adversarial UAS Activity can be used by adversaries to collect data on military readiness, movement of forces, signals intelligence, and supply chains for the military. These efforts could adversely affect the Nation's security and economic prosperity, and global commerce and stability. The Federal Government must foster sustainable, efficient, and cost-effective approaches to improving the Nation's resilience to the effects of Adversarial UAS Activity.

Sec. 2. ***Definitions***.
As used in this order:
(a) "Critical infrastructure'' means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.
(b) "Unmanned Aerial Systems (UAS)", commonly referred to as drones, are powered aerial platforms with electronics that can be autonomous or remotely controlled. The electronics can be used for collection and processing of multi-spectral imagery, radio frequency signals, and communications. Adversarial UAS can carry multiple types of payloads including biological, chemical, and radiological weapons. They can also carry munitions, incendiary devices, electromagnetic weapons, and highly conductive powders to short out electronics. Adversarial UAS can be prepositioned and coordinated to survey, monitor, damage or disrupt military installations, and critical infrastructure over large geographic areas.
(c) "National Critical Functions'' means the functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.
(d) "National Essential Functions'' means the overarching responsibilities of the Federal Government to lead and sustain the Nation before, during, and in the aftermath of a catastrophic emergency, such as a coordinated Adversarial UAS Activity on critical infrastructure that adversely affects the performance of Government.
(e) "Prepare'' and "preparedness'' mean the actions taken to plan, organize, equip, train, and exercise to build and sustain the capabilities necessary to prevent, protect against, mitigate the effects of, respond to, and recover from those threats that pose the greatest risk to the security of the Nation. These terms include the prediction and notification of impending Adversarial UAS Activity on military bases and critical infrastructure.

(f) A “Sector-Specific Agency’’ (SSA) is the Federal department or agency that is responsible for providing institutional knowledge and specialized expertise as well as leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the all-hazards environment. The SSAs are those identified in Presidential Policy Directive 21 of February 12, 2013 (Critical Infrastructure Security and Resilience).
(g) An “Adversarial UAS Activity” is any activity performed by a surveillance, reconnaissance, or weaponized UAS launched or controlled by adversarial nations, terrorist organizations or radicalized individuals. Such activity includes but is not limited to the survey of, monitoring of, surveillance, reconnaissance, or attack on National Security assets, Critical Infrastructure, National Critical Functions, or National Essential Functions.

Sec. 3. ***Policy***.
(a) It is the policy of the United States to prepare for the effects of Adversarial UAS Activity through targeted approaches that coordinate whole-of-government activities and encourage private-sector engagement. The Federal Government must provide warning of an impending Adversarial UAS Activity; protect against, respond to, and recover from the effects of Adversarial UAS Activity through public and private engagement, planning, and investment; and prevent adversarial events through deterrence, defense, and non-proliferation efforts. To achieve these goals, the Federal Government shall engage in risk-informed planning, prioritize research and development (R&D) to address the needs of critical infrastructure stakeholders, and, for adversarial threats, consult Intelligence Community assessments.
(b) To implement the actions directed in this order, the Federal Government shall promote collaboration and facilitate information sharing, including the sharing of threat and vulnerability assessments, among executive departments and agencies (agencies), the owners and operators of critical infrastructure, and other relevant stakeholders, as appropriate. The Federal Government shall also provide incentives, as appropriate, to private-sector partners to encourage innovation that strengthens critical infrastructure against the effects of Adversarial UAS Activity through the development and implementation of best practices, regulations, and appropriate guidance.

Sec. 4. ***Coordination***.
(a) The Assistant to the President for National Security Affairs (APNSA), through National Security Council staff and in consultation with the Director of the Office of Science and Technology Policy (OSTP), shall coordinate the development and implementation of executive branch actions to assess, prioritize, and manage the risks of Adversarial UAS Activity. The APNSA shall, on an annual basis, submit a report to the President summarizing progress on the implementation of this order, identifying gaps in capability, and recommending how to address those gaps.
(b) To further the Federal R&D necessary to prepare the Nation for the effects of Adversarial UAS Activity, the Director of OSTP shall coordinate efforts of agencies through the National Science and Technology Council (NSTC). The Director of OSTP, through the NSTC, shall

annually review and assess the R&D needs of agencies conducting preparedness activities for Adversarial UAS Activity, consistent with this order.

Sec. 5. *Roles and Responsibilities*.

(a) The President in consultation shall:

(i) appoint a Special Assistant to the President and Senior Director for Unmanned Aerial Systems to coordinate the whole-of-Government approach to defending the United States' National Security assets, Critical Infrastructure, National Critical Functions, or National Essential Functions from Adversarial UAS Activity.

(b) **The Secretary of Homeland Security shall**:

(i) provide the Secretary of Transportation with a list of critical installations where UAS flight exclusion zones are required to protect Federal, State, and local governments, critical infrastructure owners and operators, and other stakeholders;

(ii) provide an implementation plan to defend critical infrastructure sites from Adversarial UAS Activity in conjunction with the Department of Defense, the Department of Transportation, and the Department of Energy.

(iii) coordinate response to and recovery from the effects of Adversarial UAS Activity on critical infrastructure, in coordination with the heads of appropriate SSAs;

(iv) incorporate events that include Adversarial UAS Activity as a factor in preparedness scenarios and exercises;

(iv) maintain survivable means to provide necessary emergency information to the public during and after Adversarial UAS Activity; and

(v) in coordination with the Secretaries of Defense, Transportation, and Energy, and informed by intelligence-based threat assessments, develop quadrennial risk assessments on Adversarial UAS Activity, with the first risk assessment delivered within 1 year of the date of this order.

(b) **The Secretary of Transportation shall:**

(i) issue orders for the creation of UAS flight exclusion zones around military bases and critical infrastructure sites.

(ii) the FAA shall amend regulations to allow the military, law enforcement, and critical infrastructure owners to identify adversarial UAS, to capture, or kinetically disable or destroy UAS violating the flight exclusion zones using defenses such as frangible ammunition, net guns, lasers, and radio frequency weapons where applicable, placing the liability for collateral damage on the operator of the UAS.

(c) **The Secretary of Defense shall**:

(i) in cooperation with the heads of relevant agencies and with United States allies, international partners, and private-sector entities as appropriate, improve and develop the ability to rapidly characterize, attribute, and provide warning of Adversarial UAS Activity, through the use of space-based, airborne, and ground based sensing systems;

(ii) provide an operational plan to defend the Nation from adversarial UAS through defense and deterrence, consistent with the mission and national security policy of the Department of Defense.
(iii) conduct R&D and testing to defeat Adversarial UAS Activity on Department of Defense systems and infrastructure, improve capabilities to model and simulate the environments and effects of Adversarial UAS Activity, and develop counter-UAS technologies to protect Department of Defense systems and infrastructure from the effects of Adversarial UAS Activity to ensure the successful execution of Department of Defense missions;
(iv) review and update existing UAS and counter-UAS related standards for Department of Defense systems and infrastructure, as appropriate; share technical expertise and data regarding Adversarial UAS Activity and their potential effects with other agencies and with the private sector, as appropriate;
(vi) incorporate Adversarial UAS Activity as a factor in defense planning scenarios; and

(d**) The Secretary of Commerce shall:**
(i) provide timely and accurate operational observations, analyses, forecasts, and other products for the safe commercial use of UAS and for the deployment of counter-UAS technologies in flight exclusion zones, exclusive of the responsibilities of the Secretary of Defense set forth in subsection (c)(ii) of this section; and
(ii) use the capabilities of the Department of Commerce, the private sector, academia, and nongovernmental organizations to continuously improve standards for commercial UAS use and for counter UAS technology to protect critical infrastructure in flight exclusion zones.

(e) **The Secretary of Energy shall:**
(i) conduct early-stage R&D, develop pilot programs, and partner with other agencies and the private sector, as appropriate, to characterize the safe use of UAS and counter-UAS technology and the potential of adversarial UAS to survey, monitor or damage the electric power grid and its subcomponents, understand associated potential failure modes for the energy sector, and coordinate preparedness and mitigation measures with energy sector partners.
(ii) utilize the national laboratories to develop cost effective sensor systems for the detection of UAS, and counter-UAS technologies for deployment at critical infrastructure sites including directed energy weapons.

(f) **The Secretary of State shall:**
(i) lead the coordination of diplomatic efforts with United States allies and international partners to enhance resilience to Adversarial UAS Activity on military bases, civilian populations, and critical infrastructure; and
(ii) in coordination with the Secretary of Defense and the heads of other relevant agencies, strengthen deterrence efforts against Adversarial UAS Activity, which would reduce the likelihood of Adversarial UAS Activity on the United States or its allies and partners by limiting the availability of bioweapons, chemical weapons, incendiary devices, electromagnetic weapons, and air dropped munitions.

(g) **The Director of National Intelligence shall:**
(i) coordinate the collection, analysis, and promulgation, as appropriate, of intelligence-based assessments on adversaries' capabilities to conduct Adversarial UAS Activity and the likelihood of such activity; and
(ii) provide intelligence-based threat assessments to support the heads of relevant SSAs in the development of quadrennial risk assessments on Adversarial UAS Activity.
(h) The heads of all SSAs, in coordination with the Secretary of Homeland Security, shall enhance and facilitate information sharing with private-sector counterparts, as appropriate, to enhance preparedness for the effects of Adversarial UAS Activity, to identify and share vulnerabilities, and to work collaboratively to reduce vulnerabilities.
(i) The heads of all agencies that support National Essential Functions shall ensure that their all-hazards preparedness planning sufficiently addresses Adversarial UAS Activity, including through mitigation, response, and recovery, as directed by national preparedness policy.

Sec. 6. ***Implementation*****.**

(a) **Identifying national critical functions and associated priority critical infrastructure at greatest risk.**

(i) Within 60 days of the date of this order, the Secretary of Homeland Security, in coordination with the Secretary of the Interior, the heads of SSAs and other agencies as appropriate, shall identify and list the national critical functions and associated priority critical infrastructure systems, networks, and assets, including space-based assets that, if disrupted, could reasonably result in catastrophic national or regional effects on public health or safety, economic security, or national security. The Secretary of Homeland Security shall provide this list to the Secretary of Transportation for the creation of UAS flight exclusion zones. This list shall be updated, as necessary.

(ii) Within 60 days of the date of this order, the Secretary of Homeland Security, in coordination with the heads of other agencies as appropriate, shall, using appropriate government and private-sector standards, assess which identified critical infrastructure systems, networks, and assets are most vulnerable to the effects of Adversarial UAS Activity. The Secretary of Homeland Security shall provide this list to the President, through the APNSA. The Secretary of Homeland Security shall update this list using the results produced pursuant to subsection (b) of this section, and as necessary thereafter.

(b) **Amending Regulations and Developing Plans to Defend Critical Infrastructure**.

(i) Within 90 days of the identification described in subsection (a)(ii) of this section, the Secretary of Transportation shall amend the FAA regulations to allow the military, law enforcement, and owners of critical infrastructure to detect, capture, or destroy UAS that violate the flight exclusion zones around critical infrastructure.

(ii) Within 120 days of this order, the Secretary of Homeland Security, in coordination with the heads of SSAs and in consultation with the Director of OSTP and the heads of other appropriate agencies, shall provide a plan to protect critical infrastructure from Adversarial UAS Activity.
(iii) Within 120 days of this order, The Secretary of Defense shall provide a plan to protect the Nation from Adversarial UAS Activity launched or controlled by adversarial nations, terrorist organizations or radicalized individuals.

(iv) Within 1 year of the date of this order, the Secretary of Energy shall, utilizing the national laboratories, develop counter-UAS systems for deployment at critical infrastructure facilities to sense, interdict, disable, or destroy UAS that are violating flight exclusion zones.

(v) Within 1 year of the date of this order, and every 2 years thereafter, the Secretary of Homeland Security, in coordination with the Secretaries of Defense, Transportation, and Energy, and in consultation with the Director of OSTP, the heads of other appropriate agencies, and private-sector partners as appropriate, shall submit to the President, through the APNSA, a report that analyzes the technology options available to improve the resilience of critical infrastructure to the effects of Adversarial UAS Activity. The Secretaries of Defense, Energy, Transportation, and Homeland Security shall also identify gaps in available technologies and opportunities for future technological developments to inform R&D activities.

(c) **Strengthening critical infrastructure to withstand the effects of Adversarial UAS Activity.**

(i) Within 90 days of completing the actions directed in subsection (c)(ii) of this section, the Secretary of Homeland Security, in coordination with the Secretaries of Defense, Transportation, EPA, and Energy and in consultation with the heads of other appropriate agencies and with the private sector as appropriate, shall develop a plan to mitigate the effects of Adversarial UAS Activity on the vulnerable priority critical infrastructure systems, networks, and assets identified under subsection (a)(ii) of this section. The plan shall align with and build on actions identified in reports required by Executive Order 13800 of May 11, 2017 (Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure). The Secretary of Homeland Security shall implement those elements of the plan that are consistent with Department of Homeland Security authorities and resources, and report to the APNSA regarding any additional authorities and resources needed to complete its implementation. The Secretary of Homeland Security, in coordination with the Secretaries of Defense and Energy, shall update the plan as necessary based on results from the actions directed in subsections (b) and (c) of this section.

(ii) Within 180 days of the completion of the actions identified in sub- section (c)(i) of this section, the Secretary of Defense, in consultation with the Secretaries of Homeland Security, Transportation, and Energy, shall conduct a pilot test to harden a strategic military

installation, including infrastructure that is critical to supporting that installation, against the effects of Adversarial UAS Activity.

(iii) Within 180 days of completing the pilot test described in subsection (d)(ii) of this section, the Secretary of Defense shall report to the President, through the APNSA, regarding the cost and effectiveness of the evaluated approaches.

(e) **Improving response to Adversarial UAS Activity.**

(i) Within 180 days of the date of this order, the Secretary of Homeland Security, through the Administrator of the Federal Emergency Management Agency, in coordination with the heads of appropriate SSAs, shall review and update Federal response plans, programs, and procedures to account for the effects of Adversarial UAS Activity.
(ii) Within 180 days of the completion of actions directed by subsection (e)(i) of this section, agencies that support National Essential Functions shall update operational plans documenting their procedures and responsibilities to prepare for, protect against, and mitigate the effects of Adversarial UAS Activity.
(iii) Within 180 days of identifying vulnerable priority critical infrastructure systems, networks, and assets as directed by subsection (a)(ii) of this section, the Secretary of Homeland Security, in consultation with the Secretaries of Defense and Commerce, and the Chairman of the Federal Communications Commission, shall provide the Deputy Assistant to the President for Homeland Security and Counterterrorism and the Director of OSTP with an assessment of the effects of Adversarial UAS Activity on critical communications infrastructure, and recommend changes to operational plans to enhance national response and recovery efforts after Adversarial UAS Activity.

Sec. 7. ***General Provisions*****.**
(a) Nothing in this order shall be construed to impair or otherwise affect:
(i) the authority granted by law to an executive department or agency, or the head thereof; or
(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.
(b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.
(c) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.