SHIMP FOR PRESIDENT 2028

DRAFT EXECUTIVE ORDER

NATIONAL INFRASTRUCTURE AND DATA SECURITY

Presidential Day-One Policy Draft

Fogel G. Shimp
Independent Candidate for President - 2028
ACCOUNTABILITY | INTEGRITY | RULE OF LAW

This campaign discussion draft establishes a government-wide security initiative for federal networks and data, the electric grid, water systems, communications, transportation, energy infrastructure, data centers supporting critical services, supply chains, emergency communications, and other infrastructure essential to the United States.

EXECUTIVE ORDER

NATIONAL INFRASTRUCTURE AND DATA SECURITY

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 and National Policy.

It is the policy of the United States to protect federal information, critical infrastructure, essential public services, and sensitive systems from cyberattack, espionage, sabotage, physical attack, catastrophic failure, and dangerous foreign dependence. National infrastructure security shall be pursued while respecting constitutional rights, privacy, private property, federalism, and authorities established by Congress.

The Federal Government shall strengthen its own systems, improve coordination with critical-infrastructure owners and operators, identify single points of failure, and prepare for rapid restoration of essential services.

Sec. 2. National Critical Infrastructure Security Review.

(a) Within 30 days, the Secretary of Homeland Security shall coordinate a government-wide review with the Departments of Energy, Defense, Justice, Commerce, Transportation, Health and Human Services, Agriculture, Interior, the Environmental Protection Agency, and other appropriate agencies.

(b) Within 120 days, the review shall identify significant vulnerabilities affecting electricity, fuel, water and wastewater, telecommunications, data centers supporting critical functions, cloud services used by the Federal Government, transportation, emergency services, health systems, financial infrastructure within applicable authority, food and agriculture, and other nationally significant systems.

(c) Classified findings shall be protected, but an unclassified summary shall identify major categories of risk and national resilience priorities.

Sec. 3. Federal Cybersecurity and Zero-Trust Modernization.

(a) The Director of OMB and heads of agencies shall accelerate implementation of risk-based identity, access-control, encryption, logging, asset-management, vulnerability-management, and network-segmentation practices consistent with applicable federal cybersecurity requirements.

(b) Agencies shall identify unsupported legacy systems, end-of-life software, unmanaged internet-facing assets, privileged accounts lacking adequate controls, and other material vulnerabilities.

(c) Agencies shall prioritize remediation according to operational consequence and demonstrated threat rather than compliance paperwork alone.

Sec. 4. Federal Data Protection.

(a) Agencies shall inventory categories of sensitive federal data and identify systems whose compromise could materially harm national security, public safety, privacy, government operations, or individuals.

(b) Agencies shall strengthen encryption, access controls, authentication, audit logging, data-loss prevention, backup protection, and retention practices as appropriate to risk and law.

(c) Federal agencies shall minimize unnecessary collection and retention of personally identifiable information consistent with mission requirements and statutory obligations.

(d) Nothing in this order authorizes warrantless surveillance or access to private communications beyond authority provided by law.

Sec. 5. Data Centers Supporting Federal and Critical Functions.

(a) Agencies shall identify material dependencies on data centers, cloud infrastructure, network providers, and other computing facilities supporting federal or nationally critical functions.

(b) Reviews shall address physical security, cybersecurity, power and water dependence, backup generation, geographic concentration, foreign ownership or control risks where legally relevant, supply-chain exposure, and continuity planning.

(c) Federal security reviews shall focus on systems and services within federal authority and shall not create general federal access to private data-center customer content.

Sec. 6. Electric Grid Security.

(a) The Secretary of Energy, in coordination with the Department of Homeland Security and other appropriate authorities, shall assess cyber, physical, supply-chain, geomagnetic, severe-weather, and other material risks to electric generation and transmission.

(b) The assessment shall identify transformer shortages, critical substations, fuel dependencies, restoration bottlenecks, and long-lead-time equipment.

(c) Agencies shall coordinate with responsible regulators, States, utilities, and other owners and operators to improve resilience consistent with their respective legal authorities.

Sec. 7. Water and Wastewater Security.

(a) The Administrator of the Environmental Protection Agency and Secretary of Homeland Security shall strengthen coordination concerning cyber and physical risks to drinking-water and wastewater systems within existing statutory authority.

(b) Federal assistance shall prioritize significant vulnerabilities involving operational technology, remote access, chemical systems, backup power, communications, and emergency restoration.

(c) Agencies shall support small and rural systems that lack dedicated cybersecurity and technical personnel through existing lawful assistance programs.

Sec. 8. Telecommunications and Emergency Communications.

(a) The Secretary of Homeland Security, in coordination with Commerce and other appropriate authorities, shall review resilience of emergency communications and critical telecommunications dependencies.

(b) The review shall address network outages, cyberattack, foreign equipment risks, backup power, satellite dependencies, emergency alerting, interoperability, and restoration priorities.

(c) Federal agencies shall maintain continuity plans for communications during prolonged power or network disruption.

Sec. 9. Transportation Infrastructure Security.

(a) The Secretary of Transportation and Secretary of Homeland Security shall assess cyber and physical vulnerabilities affecting aviation, ports, rail, pipelines within applicable jurisdiction, highways, transit systems, and transportation control technologies.

(b) Agencies shall identify nationally significant single points of failure and develop mitigation and restoration priorities in cooperation with responsible owners and operators.

Sec. 10. Foreign Technology and Supply Chain Risk.

(a) The Secretaries of Commerce and Homeland Security, in coordination with Defense, Energy, and other agencies, shall identify critical infrastructure technologies for which foreign adversary control or concentrated foreign sourcing creates an unacceptable national-security risk.

(b) Agencies shall use existing lawful procurement, supply-chain-risk, investment-review, and security authorities to mitigate substantiated risks.

(c) Mitigation shall be evidence-based and tailored to actual security risks rather than nationality alone.

Sec. 11. Federal Contractor Cybersecurity.

(a) OMB and responsible agencies shall review cybersecurity requirements applicable to contractors operating federal information systems or handling sensitive federal information.

(b) Agencies shall improve verification of material security representations and establish appropriate consequences for knowingly false certifications or serious contractual noncompliance.

(c) Credible evidence of fraud, false statements, theft, unauthorized access, or other federal offenses shall be referred through appropriate lawful channels.

Sec. 12. Cyber Incident Reporting and Coordination.

(a) Federal agencies shall maintain procedures for rapid reporting and escalation of significant cyber incidents affecting federal systems.

(b) CISA and other responsible agencies shall improve lawful information sharing concerning significant threats, vulnerabilities, and incidents with critical-infrastructure partners.

(c) Information sharing shall protect privacy, civil liberties, proprietary information, classified information, and investigative integrity as required by law.

Sec. 13. Backup, Recovery, and Continuity of Operations.

(a) Agencies shall verify that mission-critical systems maintain appropriate backups, restoration procedures, offline or otherwise protected recovery capability where warranted, and tested continuity plans.

(b) Critical agencies shall periodically exercise scenarios involving ransomware, destructive malware, extended grid failure, telecommunications outage, loss of cloud services, and physical damage to key facilities.

(c) Exercises shall produce documented corrective actions and responsible implementation officials.

Sec. 14. Protection Against Ransomware and Cybercrime.

(a) The Attorney General and Secretary of Homeland Security shall strengthen coordination against ransomware, destructive cyberattacks, theft of sensitive data, extortion, botnets, and criminal infrastructure targeting the United States.

(b) Investigations shall prioritize significant threats to public safety, national security, federal systems, and critical infrastructure.

(c) Nothing in this order expands criminal liability beyond federal law or authorizes investigative techniques without required legal process.

Sec. 15. Critical Infrastructure Physical Security.

(a) Agencies shall identify opportunities within existing authority to improve protection of nationally significant facilities against sabotage, intrusion, theft, drone-related threats, and other credible physical risks.

(b) Security recommendations shall account for the nature of each facility and shall avoid unnecessary disclosure of sensitive vulnerability information.

(c) Federal cooperation with private owners and operators shall respect private property and applicable statutory limits.

Sec. 16. Artificial Intelligence and Automated Systems Security.

(a) Agencies deploying artificial intelligence or other high-impact automated systems in critical federal functions shall evaluate cybersecurity, data integrity, access control, model or system manipulation, supply-chain risk, continuity, and human oversight.

(b) No agency shall treat automated output as infallible. High-impact decisions shall retain the review and procedural safeguards required by applicable law.

Sec. 17. National Infrastructure Resilience Exercises.

(a) DHS shall coordinate periodic national-level exercises involving cascading infrastructure failures, including combinations of cyberattack, power loss, communications disruption, fuel shortage, transportation interruption, and water-system failure.

(b) Exercises shall include appropriate federal, State, local, Tribal, territorial, and private-sector participants.

(c) After-action findings shall identify concrete corrective measures, responsible entities, and implementation timelines.

Sec. 18. Public-Private Cooperation and Protection of Rights.

(a) Because much critical infrastructure is privately owned, agencies shall improve voluntary and legally authorized cooperation with owners and operators concerning threat information, resilience, incident response, and restoration.

(b) Nothing in this order compels disclosure of private customer content, authorizes censorship, or permits federal access to private systems or communications without lawful authority.

(c) Cybersecurity programs shall incorporate privacy and civil-liberties protections required by the Constitution and federal law.

Sec. 19. 180-Day National Infrastructure Security Action Plan.

(a) Within 180 days, the Secretary of Homeland Security shall submit to the President a National Infrastructure and Data Security Action Plan identifying priority vulnerabilities, responsible agencies, measurable resilience goals, and implementation deadlines.

(b) The Action Plan shall separately identify reforms requiring legislation or additional appropriations.

(c) Agencies shall report material progress every 180 days for the first 2 years.

Sec. 20. General Provisions.

(a) Nothing in this order shall impair authority granted by law to an executive department or agency, independent regulatory agency, or the functions of the Director of OMB.

(b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) Nothing in this order authorizes warrantless surveillance, censorship of lawful speech, uncompensated seizure of private property, compelled access to private communications beyond lawful authority, or circumvention of judicial process.

(d) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity against the United States, its departments, agencies, officers, employees, agents, contractors, or any other person.

THE WHITE HOUSE,

January 20, 2029.

DRAFTING NOTE

This order is designed to strengthen federal cybersecurity, critical-infrastructure resilience, data protection, emergency communications, and supply-chain security using existing executive authority. It expressly preserves constitutional protections, privacy, private property, federalism, independent regulatory authority, and judicial process. New appropriations or statutory authorities are reserved for recommendations to Congress.