NIAC Studies

The President's National Infrastructure Advisory Council (NIAC) comprises senior executives from industry and government who own and operate the critical infrastructure essential to modern life. At the President's request, NIAC members volunteer their time to study physical and cyber risks and recommend solutions that reduce risks and improve security and resilience. Members draw upon their deep experience, engage national experts, and conduct extensive research to discern the key insights that lead to practical federal solutions to complex problems. Since 2001, the NIAC has conducted more than 30 in-depth studies resulting in over 300 recommendations to improve critical infrastructure security and resilience.

2020

DEC **ACTIONABLE CYBER INTELLIGENCE: AN EXECUTIVE-LED COLLABORATIVE MODEL**
Evaluated the operational capabilities and requirements of the Critical Infrastructure Command Center (CICC) concept previously recommended by the NIAC in 2019. A fully functioning CICC will provide: a classified space where senior executives and cyber experts from the energy, financial services, and communications sectors can work collaboratively with intelligence analysts and other government staff to operationalize intelligence, provide tactical and innovative solutions, and mitigate the most pressing cyber threats in real time.

2019

DEC **TRANSFORMING THE U.S. CYBER THREAT PARTNERSHIP**
Examined how the federal government and private industry can collaborate seamlessly to manage urgent cyber risks in the most critical and highly targeted private infrastructures. The NIAC found that existing models are not sufficient to address the escalating cyber risks to critical infrastructure. It recommended a two-track approach to take immediate action while working toward a comprehensive solution.

2018

DEC **SURVIVING A CATASTROPHIC POWER OUTAGE: HOW TO ENHANCE THE CAPABILITIES OF A NATION**
Examined the nation's ability to respond to and recover from a catastrophic power outage of a magnitude beyond modern experience and exceeding prior events in severity, scale, duration, and consequence. The NIAC recommended a national approach to provide federal guidance and incentives to drive action across all levels of government, industry, communities and individuals. It also recommended better understanding the ways in which cascading failures across critical infrastructure will affect restoration and survival.

2017

MAY **FUTURE FOCUS STUDY: STRENGTHENING THE NIAC STUDY PROCESS**
Evaluated prior NIAC studies to identify ways to improve the study process, develop more actionable recommendations, and determine potential topics that could be examined in future studies. As a result of this study, the NIAC took steps to become more agile to better respond to the dynamic risk environment the nation's critical infrastructure faces.

AUG **SECURING CYBER ASSETS: ADDRESSING URGENT CYBER THREATS TO CRITICAL INFRASTRUCTURE**
Examined how federal authorities and capabilities can best be applied to improve cybersecurity of the most critical infrastructure assets. The NIAC recommended near-term, top-priority actions to prevent a major and debilitating cyber attack, including convening senior administration officials and executives in the Electricity Subsector and Financial Services and Communications Sectors, where cyber risks are clear and present and executive engagement is high.

2016

JUL **WATER SECTOR RESILIENCE**
Examined key security and resilience issues in the Water and Wastewater Systems Sector that could impact interconnected lifeline sectors. As a result, the NIAC recommended actions to highlight the criticality of water services, respond to emerging risks, and start to address the significant challenge of funding needed improvements to water and wastewater infrastructure.

2015

APR **EXECUTIVE COLLABORATION FOR THE NATION'S STRATEGIC CRITICAL INFRASTRUCTURE**
Recommended how to effectively engage CEOs in public-private partnerships by establishing a council of senior executive decision-makers from the Electricity Subsector and the Water and Wastewater Systems, Transportation Systems, Communications, and Financial Services Sectors.

JUL **TRANSPORTATION SECTOR RESILIENCE**
Examined the security and resilience of the nation's complex transportation systems, which are primarily owned and operated by the private sector and state and local governments. The study identified the urgent need to provide funding and guidance to ensure the safe, secure, reliable, and efficient movement of people and goods.

2014

NOV **CRITICAL INFRASTRUCTURE SECURITY RESILIENCE NATIONAL RESEARCH AND DEVELOPMENT PLAN**
Identified cross-sector research and development priorities and recommended how public-private partnerships could facilitate national priority investments in support of the national research and development plan called for in Presidential Policy Directive 21 (PPD-21).

2013

NOV **STRENGTHENING REGIONAL RESILIENCE**
Reviewed the challenges and successes associated with achieving regional resilience and recommended steps the federal government can take to help regions become more resilient.

NOV **IMPLEMENTATION OF EO 13636 AND PPD-21**
Addressed three primary aspects of Executive Order (EO) 13636 and PPD-21, including the revision of the National Infrastructure Protection Plan, the enhancement of information sharing between government and the private sector, and the development and adoption of the voluntary cybersecurity framework.

2012

JAN **INTELLIGENCE INFORMATION SHARING**
Examined all stages of the intelligence cycle—requirements generation, information collection, analysis, and dissemination—and made recommendations to advance bi-directional information sharing between critical infrastructure owners and operators and government.

2010

OCT **OPTIMIZATION OF RESOURCES FOR MITIGATING INFRASTRUCTURE DISRUPTIONS**
Provided a framework for how and where the infrastructure protection and resilience mission of the Department of Homeland Security can better support the broad national mission of community resilience.

OCT **A FRAMEWORK FOR ESTABLISHING CRITICAL INFRASTRUCTURE RESILIENCE GOALS**
Evaluated resilience practices in the Electricity Subsector and Nuclear Sector and developed a framework that could be applied to all critical infrastructure sectors to test and improve their resilience practices.

2009

JUL **FRAMEWORK FOR DEALING WITH DISASTERS AND RELATED INTERDEPENDENCIES**
Assessed the nation's ability to respond to and recover from major disasters that result in prolonged loss of infrastructure services expanding beyond a local area. It recommended actions to improve response and recovery.

SEP **CRITICAL INFRASTRUCTURE RESILIENCE**
Examined the steps government and industry should take to best integrate resilience and protection into a comprehensive risk-management strategy.

2008

JAN **CHEMICAL, BIOLOGICAL, AND RADIOLOGICAL EVENTS AND THE CRITICAL INFRASTRUCTURE WORKFORCE**
Examined the impact of chemical, biological, and radiological events on the critical infrastructure workforce and recommended ways to strengthen the nation's ability to respond to these events.

APR **THE INSIDER THREAT TO CRITICAL INFRASTRUCTURES**
Defined the insider threat for both physical and cyber realms, outlined obstacles to addressing this potential threat, and recommended near-term solutions to protect critical infrastructure from this threat.

OCT **CRITICAL INFRASTRUCTURE PARTNERSHIP STRATEGIC ASSESSMENT**
Assessed the effectiveness of the public-private partnership for critical infrastructure protection and identified opportunities to strengthen collaboration that will reduce risks to critical infrastructure.

2007

JAN **CONVERGENCE OF PHYSICAL AND CYBER TECHNOLOGIES AND RELATED SECURITY MANAGEMENT CHALLENGES**
Identified areas of potential control systems vulnerability and recommended policy changes to enable effective public-private partnerships to improve the cybersecurity posture of these critical infrastructure systems.

JAN **THE PRIORITIZATION OF CRITICAL INFRASTRUCTURE FOR A PANDEMIC OUTBREAK IN THE UNITED STATES**
Conducted a sector assessment survey to understand the private sector's needs and abilities during a pandemic, identified cross-sector interdependencies and how they can affect pandemic response, and recommended ways to ensure critical infrastructure workforce receives priority during such an event.

2006

APR **WORKFORCE PREPARATION, EDUCATION, AND RESEARCH**
Examined and provided recommendations on how the United States can ensure it is training the workforce needed to protect the nation's critical infrastructure and cyber systems.

JUL **PUBLIC-PRIVATE SECTOR INTELLIGENCE COORDINATION**
Recommended policy changes to improve how the Intelligence Community coordinates with critical infrastructure owners and operators. The study brought together leaders from each of the critical infrastructure sectors and representatives from the nation's key intelligence agencies and highlighted the importance of CEO engagement.

2005

OCT **SECTOR PARTNERSHIP MODEL IMPLEMENTATION**
Provided advice and recommendations for the structure, function, and implementation of the Sector Partnership Model proposed in the Interim National Infrastructure Protection Plan.

OCT **RISK MANAGEMENT APPROACHES TO PROTECTION**
Identified practices of risk quantification and modeling, risk tolerance and risk acceptance, and effective and ineffective risk management attributes.

2004

JAN **VULNERABILITY DISCLOSURE FRAMEWORK**
Provided a common understanding of, and developed standard practices for, disclosing and managing vulnerabilities in networked information systems.

JAN **CROSS SECTOR INTERDEPENDENCIES AND RISK ASSESSMENT GUIDANCE**
Identified interdependencies and examined how to coordinate incident management between the critical infrastructure sectors.

APR **BEST PRACTICES FOR GOVERNMENT TO ENHANCE THE SECURITY OF NATIONAL CRITICAL INFRASTRUCTURES**
Presented a framework for evaluating the applicability of government intervention across and within sectors and identified a number of best practices for government when considering intervention to encourage a more sustained and effective security posture.

JUL **EVALUATION AND ENHANCEMENT OF INFORMATION SHARING AND ANALYSIS**
Analyzed the current environment for information sharing and analysis across the critical infrastructure sectors and made recommendations to the federal government regarding enhancements, increased effectiveness, and broader influence across industries.

OCT **PRIORITIZING CYBER VULNERABILITIES**
Investigated the relative vulnerability of critical infrastructure sectors to cyber attack and provided recommendations to improve understanding of cyber risks and facilitate cross-sector coordination and planning.

OCT **COMMON VULNERABILITY SCORING SYSTEM**
Proposed an open and universal vulnerability scoring system with the ultimate goal of promoting a common understanding of vulnerabilities and their impact.

OCT **HARDENING THE INTERNET**
Provided recommendations to the federal government to work with industry to protect network infrastructure, computers, and devices connected to the internet.