Cybersecurity National Action Plan (Feb. 2016) AGA Synopsis

On February 9, 2016, President Obama released the Cybersecurity National Action Plan (CNAP) that takes near-term actions and puts in place a long-term strategy to enhance cybersecurity awareness and protections. According to the Administration, cybersecurity is one of the most important challenges we face as a Nation. Government, businesses, and individuals need to join together to address this challenge, and a continued partnership with the owners and operators of critical infrastructure will improve cybersecurity and enhance the Nation's resiliency.

The CNAP has multiple directives targeting increasing the Nation's public and private cybersecurity defenses. The following are CNAP highlights of greatest relevance to natural gas operations, and as noted by AGA, fall into the high-level categories of Strategic Planning, Federal Government Cybersecurity, Individual Cybersecurity, and Infrastructure Security & Resilience. AGA will continue to evaluate those initiatives that may impact the natural gas industry and monitor or become engaged as opportunities present themselves.

Strategic Planning

***Commission on Enhancing National Cybersecurity*.** The President is establishing the *Commission on Enhancing National Cybersecurity* (Commission) comprised of top strategic, business, and technical thinkers from outside of Government – including bi-partisan representation from Congressional leadership. The Commission will report to the President with specific findings and recommendations before the end of 2016, providing the country a roadmap for future actions that enhance cybersecurity awareness and protections throughout the private sector and at all levels of Government. The National Institute of Standards and Technology (NIST) will provide the Commission with support.

Federal Cybersecurity

***Federal Chief Information Security Officer*.** The Administration has created the position of Federal Chief Information Security Officer to drive cybersecurity policy, planning, and implementation across the Federal Government. This will include proposed increased funding for Information Technology Modernization – retiring, replacing, or modernizing antiquated Federal Government IT infrastructure, networks, and systems.

Federal Cybersecurity Programs. The Administration is expanding existing Federal cybersecurity programs such as the Department of Homeland Security's EINSTEIN and Continuous Diagnostics and Mitigation programs. Across all Federal agencies there will be a coordinated approach to government-wide shared services for IT and cybersecurity. Government funding is proposed for enhancing cybersecurity education and training nationwide and hire more cybersecurity experts to secure Federal agencies.

Cybersecurity National Action Plan (Feb. 2016) AGA Synopsis

Individual Cybersecurity

Identity Theft. The Federal government will expand the campaign to protect against identity theft. A new program will be established that will better protect and secure the data and personal information of Americans as they interact with Federal Government services, including tax data and benefit information. There will be greater emphasis within the government and across the private sector for the use of multi-factor authentication. And there will be relaunching awareness campaigns and tools available to the general public regarding identify theft, countermeasures, and recovery.

Enhance Critical Infrastructure Security and Resilience

Security Testing. DHS, the Department of Commerce (DOC), and the Department of Energy are contributing resources and capabilities to establish a *National Center for Cybersecurity Resilience*, where companies and sector-wide organizations can test the security of systems in a contained environment, such as by subjecting a replica electric grid to cyber-attack.

Additional Intellectual Resources. DHS will double the number of cybersecurity advisors available to assist private sector organizations with in-person, customized cybersecurity assessments and implementation of best practices.

Network Cyber Integrity. DHS is collaborating with UL and other industry partners to develop a *Cybersecurity Assurance Program* to test and certify networked devices within the "Internet of Things," whether they be refrigerators or medical infusion pumps, so that new products with cyber-based components can be certified to meet security standards.

Cybersecurity Framework. NIST is continuing to solicit feedback to inform further development of the Cybersecurity Framework for improving critical infrastructure cybersecurity.

Cyber R&D. The Administration is releasing its *2016 Federal Cybersecurity Research and Development Strategic Plan* intended to lay out strategic R&D goals for the Nation to advance cybersecurity technologies. DOC has also established the *National Cybersecurity Center of Excellence*, a public-private research and development partnership that will allow industry and government to work together to develop and deploy technical solutions for high-priority cybersecurity challenges.

Government Reconnaissance. The Department of Justice, including the Federal Bureau of Investigation, is increasing funding for cybersecurity-related activities by more than 23 percent to improve their capabilities to identify, disrupt, and apprehend malicious cyber actors.

Cyber Incident Response. In spring 2016, the Administration will publicly release a policy for national cyber incident coordination and an accompanying severity methodology for evaluating cyber incidents so that government agencies and the private sector can communicate effectively and provide an appropriate and consistent level of response.

FACT SHEET: Cybersecurity National Action Plan
Taking bold actions to protect Americans in today's digital world

From the beginning of his Administration, the President has made it clear that cybersecurity is one of the most important challenges we face as a Nation, and for more than seven years he has acted comprehensively to confront that challenge. Working together with Congress, we took another step forward in this effort in December with the passage of the Cybersecurity Act of 2015, which provides important tools necessary to strengthen the Nation's cybersecurity, particularly by making it easier for private companies to share cyber threat information with each other and the Government.

But the President believes that more must be done – so that citizens have the tools they need to protect themselves, companies can defend their operations and information, and the Government does its part to protect the American people and the information they entrust to us. That is why, today, the President is directing his Administration to implement a **Cybersecurity National Action Plan (CNAP)** that takes near-term actions and puts in place a long-term strategy to enhance cybersecurity awareness and protections, protect privacy, maintain public safety as well as economic and national security, and empower Americans to take better control of their digital security.

The Challenge

From buying products to running businesses to finding directions to communicating with the people we love, an online world has fundamentally reshaped our daily lives. But just as the continually evolving digital age presents boundless opportunities for our economy, our businesses, and our people, it also presents a new generation of threats that we must adapt to meet. Criminals, terrorists, and countries who wish to do us harm have all realized that attacking us online is often easier than attacking us in person. As more and more sensitive data is stored online, the consequences of those attacks grow more significant each year. Identity theft is now the fastest growing crime in America. Our innovators and entrepreneurs have reinforced our global leadership

Source: The White House, Office of the Press Secretary, February 09, 2016

and grown our economy, but with each new story of a high-profile company hacked or a neighbor defrauded, more Americans are left to wonder whether technology's benefits could risk being outpaced by its costs.

The President believes that meeting these new threats is necessary and within our grasp. But it requires a bold reassessment of the way we approach security in the digital age. If we're going to be connected, we need to be protected. We need to join together—Government, businesses, and individuals—to sustain the spirit that has always made America great.

Our Approach

That is why, today, the Administration is announcing a series of near-term actions to enhance cybersecurity capabilities within the Federal Government and across the country. But given the complexity and seriousness of the issue, the President is also asking some of our Nation's top strategic, business, and technical thinkers from outside of government to study and report on what more we can do to enhance cybersecurity awareness and protections, protect privacy, maintain public safety as well as economic and national security, and empower Americans to take better control of their digital security. Bold action is required to secure our digital society and keep America competitive in the global digital economy.

The President's **Cybersecurity National Action Plan (CNAP)** is the capstone of more than seven years of determined effort by this Administration, building upon lessons learned from cybersecurity trends, threats, and intrusions. This plan directs the Federal Government to take new action now and fosters the conditions required for long-term improvements in our approach to cybersecurity across the Federal Government, the private sector, and our personal lives. Highlights of the CNAP include actions to:

- **Establish the "Commission on Enhancing National Cybersecurity."** This Commission will be comprised of top strategic, business, and technical thinkers from outside of Government – including members to

be designated by the bi-partisan Congressional leadership. The Commission will make recommendations on actions that can be taken over the next decade to strengthen cybersecurity in both the public and private sectors while protecting privacy; maintaining public safety and economic and national security; fostering discovery and development of new technical solutions; and bolstering partnerships between Federal, State, and local government and the private sector in the development, promotion and use of cybersecurity technologies, policies, and best practices.

- Modernize Government IT and transform how the Government manages cybersecurity through the proposal of a $3.1 billion Information Technology Modernization Fund, which will enable the retirement, replacement, and modernization of legacy IT that is difficult to secure and expensive to maintain, as well as the formation of a new position – the **Federal Chief Information Security Officer** – to drive these changes across the Government.
- Empower Americans to secure their online accounts by moving beyond just passwords and adding an extra layer of security. By judiciously combining a strong password with additional factors, such as a fingerprint or a single use code delivered in a text message, Americans can make their accounts even more secure. This focus on multi-factor authentication will be central to a new National Cybersecurity Awareness Campaign launched by the National Cyber Security Alliance designed to arm consumers with simple and actionable information to protect themselves in an increasingly digital world. The National Cyber Security Alliance will partner with leading technology firms like Google, Facebook, DropBox, and Microsoft to make it easier for millions of users to secure their online accounts, and financial services companies such as MasterCard, Visa, PayPal, and Venmo that are making transactions more secure. In addition, the Federal Government will take steps to safeguard personal data in online transactions between citizens and the government, including through a new action plan to drive the Federal Government's adoption and use of effective identity proofing and strong multi-factor authentication methods and a systematic review of where the Federal Government can reduce reliance on Social Security Numbers as an identifier of citizens.
- Invest over $19 billion for cybersecurity as part of the President's Fiscal Year (FY) 2017 Budget. This represents a more than 35 percent

increase from FY 2016 in overall Federal resources for cybersecurity, a necessary investment to secure our Nation in the future.

Through these actions, additional new steps outlined below, and other policy efforts spread across the Federal Government, the Administration has charted a course to enhance our long-term security and reinforce American leadership in developing the technologies that power the digital world.

Commission on Enhancing National Cybersecurity

For over four decades, computer technology and the Internet have provided a strategic advantage to the United States, its citizens, and its allies. But if fundamental cybersecurity and identity issues are not addressed, America's reliance on digital infrastructure risks becoming a source of strategic liability. To address these issues, we must diagnose and address the causes of cyber-vulnerabilities, and not just treat the symptoms. Meeting this challenge will require a long-term, national commitment.

To conduct this review, the President is establishing the **Commission on Enhancing National Cybersecurity**, comprised of top strategic, business, and technical thinkers from outside of Government – including members to be designated by the bi-partisan Congressional leadership. The Commission is tasked with making detailed recommendations on actions that can be taken over the next decade to enhance cybersecurity awareness and protections throughout the private sector and at all levels of Government, to protect privacy, to maintain public safety and economic and national security, and to empower Americans to take better control of their digital security. The National Institute of Standards and Technology will provide the Commission with support to allow it to carry out its mission. The Commission will report to the President with its specific findings and recommendations before the end of 2016, providing the country a roadmap for future actions that will build on the CNAP and protect our long-term security online.

Raise the Level of Cybersecurity across the Country

While the Commission conducts this forward looking review, we will continue to raise the level of cybersecurity across the Nation.

Strengthen Federal Cybersecurity

The Federal Government has made significant progress in improving its cybersecurity capabilities, but more work remains. To expand on that progress and address the longstanding, systemic challenges in Federal cybersecurity, we must re-examine our Government's legacy approach to cybersecurity and information technology, which requires each agency to build and defend its own networks. These actions build upon the foundation laid by the **Cybersecurity Cross-Agency Priority Goals** and the **2015 Cybersecurity Strategy and Implementation Plan**.

- The President's 2017 Budget proposes a $3.1 billion Information Technology Modernization Fund, as a down payment on the comprehensive overhaul that must be undertaken in the coming years. This revolving fund will enable agencies to invest money up front and realize the return over time by retiring, replacing, or modernizing antiquated IT infrastructure, networks, and systems that are expensive to maintain, provide poor functionality, and are difficult to secure.
- The Administration has created the position of Federal Chief Information Security Officer to drive cybersecurity policy, planning, and implementation across the Federal Government. This is the first time that there will be a dedicated senior official who is solely focused on developing, managing, and coordinating cybersecurity strategy, policy, and operations across the entire Federal domain.
- The Administration is requiring agencies to identify and prioritize their highest value and most at-risk IT assets and then take additional concrete steps to improve their security.
- The Department of Homeland Security, the General Services Administration, and other Federal agencies will increase the availability of government-wide shared services for IT and cybersecurity, with the goal of taking each individual agency out of the business of building, owning, and operating their own IT when more efficient, effective, and secure options are available, as well as ensuring that individual agencies are not left on their own to defend themselves against the most sophisticated threats.

Source: The White House, Office of the Press Secretary, February 09, 2016

- The Department of Homeland Security is enhancing Federal cybersecurity by expanding the EINSTEIN and Continuous Diagnostics and Mitigation programs. The President's 2017 Budget supports all Federal civilian agencies adopting these capabilities.
- The Department of Homeland Security is dramatically increasing the number of Federal civilian cyber defense teams to a total of 48, by recruiting the best cybersecurity talent from across the Federal Government and private sector. These standing teams will protect networks, systems, and data across the entire Federal Civilian Government by conducting penetration testing and proactively hunting for intruders, as well as providing incident response and security engineering expertise.
- The Federal Government, through efforts such as the National Initiative for Cybersecurity Education, will enhance cybersecurity education and training nationwide and hire more cybersecurity experts to secure Federal agencies. As part of the CNAP, the President's Budget invests $62 million in cybersecurity personnel to:
    - Expand the Scholarship for Service program by establishing a CyberCorps Reserve program, which will offer scholarships for Americans who wish to obtain cybersecurity education and serve their country in the civilian Federal government;
    - Develop a Cybersecurity Core Curriculum that will ensure cybersecurity graduates who wish to join the Federal Government have the requisite knowledge and skills; and,
    - Strengthen the **National Centers for Academic Excellence in Cybersecurity Program** to increase the number of participating academic institutions and students, better support those institutions currently participating, increase the number of students studying cybersecurity at those institutions, and enhance student knowledge through program and curriculum evolution.
- The President's Budget takes additional steps to expand the cybersecurity workforce by:
    - Enhancing student loan forgiveness programs for cybersecurity experts joining the Federal workforce;
    - Catalyzing investment in cybersecurity education as part of a robust computer science curriculum through **the President's Computer Science for All Initiative**.

Source: The White House, Office of the Press Secretary, February 09, 2016

Empower Individuals

The privacy and security of all Americans online in their daily lives is increasingly integral to our national security and our economy. The following new actions build on the President's **2014 BuySecure Initiative** to strengthen the security of consumer data.

- The President is calling on Americans to move beyond just the password to leverage multiple factors of authentication when logging-in to online accounts. Private companies, non-profits, and the Federal Government are working together to help more Americans stay safe online through a new public awareness campaign that focuses on broad adoption of multi-factor authentication. Building off the Stop.Think.Connect. campaign and efforts stemming from the National Strategy for Trusted Identities in Cyberspace, the National Cyber Security Alliance will **partner with leading technology companies and civil society** to promote this effort and make it easier for millions of users to secure their accounts online. This will support a broader effort to increase public awareness of the individual's role in cybersecurity.
- The Federal Government is accelerating adoption of strong multi-factor authentication and identity proofing for citizen-facing Federal Government digital services. The General Services Administration will establish a new program that will better protect and secure the data and personal information of Americans as they interact with Federal Government services, including tax data and benefit information.
- The Administration is conducting a systematic review of where the Federal Government can reduce its use of Social Security Numbers as an identifier of citizens.
- The Federal Trade Commission recently relaunched **IdentityTheft.Gov**, to serve as a one-stop resource for victims to report identity theft, create a personal recovery plan, and print pre-filled letters and forms to send to credit bureaus, businesses, and debt collectors.
- The Small Business Administration (SBA), partnering with the Federal Trade Commission, the National Institute of Standards and Technology (NIST), and the Department of Energy, will offer cybersecurity training to reach over 1.4 million small businesses and small business stakeholders through 68 SBA District Offices, 9 NIST Manufacturing Extension Partnership Centers, and other regional networks across the

country.
- The Administration is announcing new milestones in **the President's BuySecure Initiative** to secure financial transactions. As of today the Federal Government has supplied over 2.5 million more secure Chip-and-PIN payment cards, and transitioned to this new technology the entire fleet of card readers managed by the Department of the Treasury. Through government and private-sector leadership, more secure chip cards have been issued in the United States than any other country in the world.

Enhance Critical Infrastructure Security and Resilience

The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure. A continued partnership with the owners and operators of critical infrastructure will improve cybersecurity and enhance the Nation's resiliency. This work builds off the President's previous cybersecurity focused Executive Orders on **Critical Infrastructure** (2013) and **Information Sharing** (2015).

- The Department of Homeland Security, the Department of Commerce, and the Department of Energy are contributing resources and capabilities to establish a National Center for Cybersecurity Resilience where companies and sector-wide organizations can test the security of systems in a contained environment, such as by subjecting a replica electric grid to cyber-attack.
- The Department of Homeland Security will double the number of cybersecurity advisors available to assist private sector organizations with in-person, customized cybersecurity assessments and implementation of best practices.
- The Department of Homeland Security is collaborating with UL and other industry partners to develop a Cybersecurity Assurance Program to test and certify networked devices within the "Internet of Things," whether they be refrigerators or medical infusion pumps, so that when you buy a new product, you can be sure that it has been certified to meet security standards.
- The National Institute of Standards and Technology is **soliciting feedback** in order to inform further development of its Cybersecurity Framework for improving critical infrastructure cybersecurity. This

follows two years of adoption by organizations across the country and around the world.
- Yesterday, Commerce Secretary Pritzker cut the ribbon on the new **National Cybersecurity Center of Excellence**, a public-private research and development partnership that will allow industry and government to work together to develop and deploy technical solutions for high-priority cybersecurity challenges and share those findings for the benefit of the broader community.
- The Administration is calling on major health insurers and healthcare stakeholders to help them take new and significant steps to enhance their data stewardship practices and ensure that consumers can trust that their sensitive health data will be safe, secure, and available to guide clinical decision-making.

Secure Technology

Even as we work to improve our defenses today, we know the Nation must aggressively invest in the science, technology, tools, and infrastructure of the future to ensure that they are engineered with sustainable security in mind.

- Today the Administration is releasing its **2016 Federal Cybersecurity Research and Development Strategic Plan**. This plan, which was called for in the 2014 Cybersecurity Enhancement Act, lays out strategic research and development goals for the Nation to advance cybersecurity technologies driven by the scientific evidence of efficacy and efficiency.
- In addition, the Government will work with organizations such as the Linux Foundation's Core Infrastructure Initiative to fund and secure commonly used internet "utilities" such as open-source software, protocols, and standards. Just as our roads and bridges need regular repair and upkeep, so do the technical linkages that allow the information superhighway to flow.

Deter, Discourage, and Disrupt Malicious Activity in Cyberspace

Better securing our own digital infrastructure is only part of the solution. We must lead the international effort in adopting principles of

responsible state behavior, even while we take steps to deter and disrupt malicious activity. We cannot pursue these goals alone – we must pursue them in concert with our allies and partners around the world.

- In 2015, members of the G20 joined with the United States in affirming important norms, including the applicability of international law to cyberspace, the idea that states should not conduct the cyber-enabled theft of intellectual property for commercial gain, and in welcoming the report of a United Nations Group of Governmental Experts, which included a number of additional norms to promote international cooperation, prevent attacks on civilian critical infrastructure, and support computer emergency response teams providing reconstitution and mitigation services. The Administration intends to institutionalize and implement these norms through further bilateral and multilateral commitments and confidence building measures.
- The Department of Justice, including the Federal Bureau of Investigation, is increasing funding for cybersecurity-related activities by more than 23 percent to improve their capabilities to identify, disrupt, and apprehend malicious cyber actors.
- U.S. Cyber Command is building a Cyber Mission Force of 133 teams assembled from 6,200 military, civilian, and contractor support personnel from across the military departments and defense components. The Cyber Mission Force, which will be fully operational in 2018, is already employing capabilities in support of U.S. Government objectives across the spectrum of cyber operations.

Improve Cyber Incident Response

Even as we focus on preventing and deterring malicious cyber activity, we must also maintain resilience as events occur. Over the past year, the country faced a wide array of intrusions, ranging from criminal activity to cyber espionage. By applying lessons learned from past incidents we can improve management of future cyber incidents and enhance the country's cyber-resilience.

- By this spring, the Administration will publicly release a policy for national cyber incident coordination and an accompanying severity

methodology for evaluating cyber incidents so that government agencies and the private sector can communicate effectively and provide an appropriate and consistent level of response.

Protect the Privacy of Individuals

In coordination with the information technology and cybersecurity efforts above, the Administration has launched a groundbreaking effort to enhance how agencies across the Federal Government protect the privacy of individuals and their information. Privacy has been core to our Nation from its inception, and in today's digital age safeguarding privacy is more critical than ever.

- Today, the President signed an Executive Order that created a permanent **Federal Privacy Council**, which will bring together the privacy officials from across the Government to help ensure the implementation of more strategic and comprehensive Federal privacy guidelines. Like cyber security, privacy must be effectively and continuously addressed as our nation embraces new technologies, promotes innovation, reaps the benefits of big data and defends against evolving threats.

Fund Cybersecurity

In order to implement these sweeping changes, the Federal Government will need to invest additional resources in its cybersecurity. That is why the 2017 Budget allocates more than $19 billion for cybersecurity – a more than 35 percent increase over the 2016 enacted level. These resources will enable agencies to raise their level of cybersecurity, help private sector organizations and individuals better protect themselves, disrupt and deter adversary activity, and respond more effectively to incidents.

###

Source: The White House, Office of the Press Secretary, February 09, 2016