The Internet Of Things Poses A Vast Security Threat To The Federal Workforce's Network

Benjamin Evans, Morgan Meek, and Ryan Restivo

24 April 2015

The Internet of Things (IoT) introduces vulnerable gateways and a significant security threat to the federal network that may be mitigated through establishing one regulatory force such as the Federal Communications Commission (FCC), a policy making body that establishes policy proactively in order to influence the design of IoT devices. The benefits to having a regulatory force such as the FCC are that it: already is a regulator of similar technology,[1] has the ability to influence IoT designs via regulatory policy in order to establish security requirements, has the capability to act as a single control point for IoT implementation, and has the capability to exercise its established educational program to promote a methodical integration of the IoT into the federal network. The IoT is the extension of the Internet to objects other than computers.[2] Devices that fall under the umbrella of the IoT include anything that can be assigned an ip address.[3] Smart TVs, lights, cars, doors, supply chains, and thermostats are just a few of the objects that are beginning to use IoT technology in some of their hardware components while simultaneously becoming vulnerable gateways into the federal network, just so long as the government does not influence their design via policy.[4]

The data becoming available via the use IoT technologies is expanding at an exponential rate to both the public and private sector. CISCO expects 400 zettabytes of information (400 billion terabytes, over 10 TB per human on the planet) to have been recorded by 2020.[14] The U.S is among the leaders of nations recording data at that rate, and a large portion of that data is sensitive information such as credit card information, medical history, bank accounts, government projects etc. The data that IoT devices are collecting for U.S government application also has implications for effectively managing public works, roads, infrastructure, worker efficiency, city planning, rail systems, etc. Through hardware instrumentation connected to the IoT, nearly every manageable resource can provide unique information to aid in governance but also presents avenues of approach for attackers leaving critical infrastructure and big data at risk. Imagine a cyber attacker wishing to do damage to the United States' critical infrastructure connecting to an IoT device that has a function within the power grid. An attacker may do catastrophic damage, collect an incredible amount of intelligence, or use these devices as gateways to deeper information stored in the government's big data. These threatening implications establish the significance of the problem that unregulated, poorly secure, or unsecured IoT devices pose to the federal workforce's network.

Furthermore, the lack of regulation of IoT devices is a very significant issue for the federal workforce as these IoT devices are implemented into the federal workforce's network and as "smart" technologies connect to the federal network. In the private sector,

companies are developing devices that connect to the internet in order to provide more convenience to the customer. For example, a customer can adjust the temperature of their house remotely if they have a “smart” thermostat that is connected to the internet. Due to the fact that this technology provides more convenience to users, it without a doubt will continue to develop and integrate into everyday life. While these “smart” devices are exciting for users, they pose threats to the networks they are connected to, for they are unsecured gateways into the network. This creates a problem as the IoT is integrated into the federal workforce and when these devices begin to connect to the government’s networks because attackers trying to access the government’s big data will have easier entrances into the network. Currently, there are virtually no government regulations dictating the security requirements or capability restrictions that these devices may need for successful integration, thus leaving the growing number of nodes on the federal network unsecured and open for penetration by hackers. Currently, no federal law comprehensively governs privacy and security of personal information in regards to IoT technologies, though several government organizations have begun to assess the need for some regulation.[10] In November of 2013, the Federal Trade Commission discussed the security concerns but ultimately did not develop any plan for regulation.[10]

Additionally, maintaining reactionary policy is a danger to the federal network, so having a proactive strategy in securing the federal workforce’s network in regards to IoT technology is vital to ensuring information security. An example of a reactionary policy that addresses developing security concerns is the U.S Army’s establishment of a cyber branch. The increasing need for the cyber branch also gives rise to the growing influence that the US has over the policy concerning the production of the IoT technologies. With those technologies being produced faster than policy can be written, the branch also has the duty to help detect and prevent attacks on the federal system. Hand-in-hand with this protection comes the counterattack obligation to trace the threat back to the source and properly shut it down. Despite these benefits provided by the Cyber branch, they come at a price that taxpayers are left to pay. It can be very expensive to train the soldiers needed to run the systems and man the monitoring stations. This coupled with the cost of the equipment and the programs needed to create the system and the cost of keeping these systems running all the time, can initially appear to be an overwhelming price. This is the epitome of a costly and reactionary policy in response to the growing security concerns brought about by the development and implementation of new technologies such as IoT devices. If the U.S government is going to develop a proactive strategy in defending against various security threats than, it may need to develop policies from one regulating entity that influence the production of these devices. This may facilitate a drastic decrease in the number of unsecured IoT devices on the internet that may be used to threaten the government’s big data or critical infrastructure.

There are many megatrends shaping the world of Cyber security, and it is important to not view security breaches as simply events but rather parts of a larger more holistic megatrend. Over the course of time, a megatrend that has occurred in the relationship between hackers and their victims is that when a target solidifies their network defenses, a hacker will develop a more complex attack that approaches from a different avenue of approach in order to gain access. The victim then secures the vulnerability, and the reinforcing cycle repeats itself. With more unsecured or poorly secured nodes on the federal network, man in the middle attacks, brute force denial of service attacks, and exploits will all become more complex, catastrophic and easier for hackers to conduct. If no action is taken to influence the long term strategic implementation of IoT via policy that influences IoT technology design and production, then the federal workforce cannot successfully adopt and implement the IoT without accepting too much risk of data being compromised or critical assets being exposed, and securing data is a primary concern to the American public as well as an asset for global competitiveness. An interesting example of how the IoT may possibly lead to the comprising of data is the recent cyber attack conducted on Anthem, a leading American insurance company, and while Anthem is not the federal workforce, what happened to this private company may very well happen to the federal workforce. Recently,a network security breach put 80 million people's data at risk of being compromised.[5] All the necessary actions that Anthem had to take following the attack such as mailing out 80 million letters, paying for a year's worth identity theft protection for 80 million people, and hiring cyber forensic companies to investigate the attack has cost the Anthem Corporation over $40 million dollars so far.[5] It is suspected that this attack occurred because a poorly secured cyber-physical device of the data center's infrastructure such as a temperature sensor or a network connected HVAC controller was exploited as a poorly defended gateway into the network. These "HVAC systems and mobile apps that allow remote control lighting or building operations can also open those systems to cyber attacks or manipulation, presenting new layers of electronic vulnerabilities."[6] The IoT introduces a plethora of security challenges, and due to the fact that there are already regulating bodies for other technologies such as the FCC who already deals with cell phones, establishing one regulating body may mitigate some of these security risks.

As the public realizes that IoT is a threat to sensitive information and the government begins to influence the design of IoT products, the security concerns would be high in the globally competitive market. the resulting environment may be one where there is high security requirements for IoT technologies leading to a global adoption of IoT technology. Global investment of the technology may continue to rise as implementation in both public and private sectors in the United States rises. Security protocol of hardware is well established and enforced as data collection becomes nearly ubiquitous. Big data collection has risen to 400 zettabytes (400 billion terabytes) and far exceeds the amount of information any organization can reasonably process.[14] Data consumers of all kinds focus

on collecting more timely, relevant data for decision making. Foreign adversaries may not remain a threat in the global competitive market or continue to conduct sophisticated and targeted attacks without developing new strategies to navigate around the security protocols established. Without government influence on the manner in which these IoT devices connect to government and private systems, the growing security vulnerabilities make these devices a liability instead of an asset because they become new passageways for attackers. The government can proactively be taking an intentional effort to influence the actual designs of these IoT devices in order to ensure that they have the proper security capabilities required of a federal workforce device. There are many simple attacks even an entry level hacker can complete with unsecure or weakly secure devices to include eavesdropping, denial of service attacks, or identity spoofing. The ease of these attacks simply increases the threat of the attacks because they do not require any type of specific training, thus further supporting the argument that a regulatory force is needed. While some may argue that a single regulatory force has some unintended consequences that come along with it such as “Bigger Government” as some conservatives would put it, regulating the security requirements of IoT devices is just the Government extending its pursuit of national defense to the newest domain of the battlefield, Cyber.

The FCC is an example of a regulatory force that could serve as the single control point for IoT technologies due to the fact that the FCC already regulates similar devices such as cell phones successfully but it has limited authority over IoT policy and regulation.[7] It is important to note that the argument is not for the FCC being the regulating body, but rather just giving an example of a strategy that could be implemented or be used a guide when developing another strategy. The FCC has a history of regulatory practices especially regarding cellphones to specifically deal with compliance issues. All communication devices produced and consumed in the United States must comply to the federal regulations to secure how information is received, and this also extends to peripheral devices[1]. Governmental classification of IoT hardware as a communication device peripheral due to the fact that it produces transmission noise/sends data packets may largely place an existing infrastructure of regulation upon the emerging technology. This classification can be authorized by FCC code and due to IoT hardware feeding data to a larger network.[8] Examples of threats due to no regulation are seen in countries without a regulatory system in place to control data transmitting devices. Without specific control and enforcement, devices can more freely connect to other devices such as phones or networks where no minimum security settings are required. This is akin to not requiring a password on an email account, anyone with interest may have access with the right knowledge. IoT devices are no different in structure of communication with regards to packet transmission. A government system without enforced regulation may expose networks to a denial of service or data loss.

The FCC or another regulating body may influence the design of IoT devices to have certain security specifications through a strong regulatory policy in order to successfully implement the IoT into the federal workforce without compromising the security of the federal network. If the regulating body proactively begins to influence the private sector in the production of IoT technologies in order to accommodate the security requirements they deem necessary, then the federal workforce will successfully implement the IoT without sacrificing convenience and security in a globally competitive market. The federal government can have an influence on the production of the products from the introduction of the technology through R&D, contracted work, sales to government, and grants, all with a goal of secure data and assets as an investment as well as legislation.[9] This strategy is proactive in securing data before governance gaps force reactionary policy and reactionary federal network security strategies. Private sector manufacturers will develop products around the preemptively established security requirements without compromising government needs. The U.S government owes it to its people to protect their communications and close any security vulnerabilities threatening the integrity of their data. The government should consider the use of big data because a failure to adopt it will result in a strategic disadvantage against global competitors thus establishing the need for the government to create policy that influences the production of these IoT devices.

A regulatory force for IoT technology is needed because IoT technology has not even been classified by any regulatory system of the United States government in order to govern its use explicitly.[10] The classification of the technology largely affects how it can be regulated and how much funding will be required to maintain the regulation due to the evolving nature of the technology. With the implementation of the IoT over the next 20 years, the FCC or another regulating entity may expand its criteria for communication devices to be anything that makes transmission noise and/or sends data packets via a transmission protocol.[8] The Department of Homeland Security (DHS) or some enforcing body may then be allowed to enforce these new policies under the regulating organization's guidance. This may mean, as our hypothesis dictates, that the government, (through the a regulating body expanding its range of authority) through policy, may regulate the IoT devices by deeming what the devices must have in regards to security protocols and capabilities in general, and the companies making the IoT devices may be required by law to make their devices with those specific protocols.[11] The proposed scenario falls under the hypothesis because it is the government developing policy that influences the production of IoT devices in their developmental stages. This scenario may be viewed as the U.S government patching holes in U.S big data security vulnerabilities in order to ensure the liberty of the U.S people to communicate as they please without fear of data being compromised. It may be viewed as the U.S government protecting its people by strengthening its cyber national security versus the idea that the U.S government may be infringing upon the free market. In this scenario, the government is not censoring or

controlling the communications on the internet, but rather hardening the defenses around them.

Having a regulatory force such as the FCC to develop the policies influencing the IoT may establish a single control point to lead the integration of the IoT into the federal workforce. The regulator may introduce IoT regulation in stages that coincides with the projected development of IoT in the integration into the federal workforce versus the current piecemeal integration that occurs as technologies are developed. By an organization becoming the single control point, it may allow the integration to become a more controlled process thus enabling the implementation of the IoT into the federal workforce in stages. There are eight steps that an organization may do systematically in order to successfully implement the IoT successfully in stages (refer to Appendix F for more details). IT security is commonly referred to as an onion with multiple layers of security where each layer of the onion has a generally understood acceptable amount of assumed risk that may be allowed. As the federal workforce implements the IoT and allows these technologies to have access to their systems via the single control point of the a regulating body, the federal workforce would likely first harden their security protocols on their infrastructure systems because the risk of attack via infrastructure devices is higher as attackers use these unsecured or poorly secured infrastructure systems as a means to reach the critical and non critical systems. Infrastructure provides the environmentals for the devices that store and control big data, so if those are compromised then there are a lot of negative implications such as the higher risk of cyber sabotage. Furthermore, the federal workforce likely would then allow the IoT technologies to touch the non critical systems first, for these non critical systems are the development areas. This will allow the federal workforce the opportunity to establish best practices, identify vulnerabilities, and develop mitigation measures. Upon successful implementation of the IoT into the non critical development environments, then the federal workforce would likely then implement the IoT into the critical production environments. This sequence will allow for the most secure implementation of the IoT into the federal networks system, but this will only be possible if a regulating entity is established as the single control point controlling the flow and process of the IoT integration into the federal workforce. (refer to Appendix B for more details)

When establishing a regulating entity in regards to IoT it is important to consider the ways that education can be used to mitigate security threats. For example, FCC has workshops in place in order to provide education about certain technologies within their span of control.[12] The purpose of establishing an IoT specific education program may be to ensure training of public and private employees in methodological integration and systems uses. When employees know the capabilities of their systems and what vulnerabilities exist, it will be easier to monitor systems from the everyday user. Acceptance of the technology is a side effect of education in promoting efficiency in the

government workforce. Without education the end user may inadvertently cause damage to the existing network or increase its vulnerability. Education of computer systems have been shown to prevent costly setbacks to computer systems in the government network. Simple attacks such as social engineering employees to plug in infected USB drives results in damage that may be easily preventable with education.

The Internet of Things (IoT) introduces vulnerable gateways and a significant security threat to the federal network that may be mitigated through establishing one regulatory force such as the Federal Communications Commission (FCC), a policy making body that establishes policy proactively in order to influence the design of IoT devices. The benefits to having a regulatory force such as the FCC are that it: already is a regulator of similar technology,[1] has the ability to influence IoT designs via regulatory policy in order to establish security requirements, has the capability to act as a single control point for IoT implementation, and has the capability to exercise its established educational program to promote a methodical integration of the IoT into the federal network. The implication of the growing number of security vulnerabilities due to the IoT is that the data of the United States people, credit card information, health information, personal internet traffic, classified defense information and critical infrastructure such as the power grid, water lines etc. will all become more accessible to attackers. A strategy that the United States government may take to mitigate these security vulnerabilities, is to influence the production of IoT devices via regulatory policy established by a regulator and allow an agency such as the DHS to enforce the regulations. This may simply require that the policy makers expand what a pre existing organization such as FCC is allowed to regulate to be anything that sends a data packet and/or anything that makes any type of transmission noise,[13] but it also might require the establishment of a new organization. The IoT is an exciting accomplishment in technological advancement that should be celebrated, but the United States government must develop the proper long term strategies in order to prevent the IoT from threatening its national security.

Endnotes

1. U.S. Federal Communications Commision, *What We Do* Accessed April 3, 2015. http://www.fcc.gov/what-we-do.

2. Turk, Victoria. "The Internet of Things Has a Language Problem." Motherboard. July 18, 2014. Accessed December 2, 2014. http://motherboard.vice.com/read/the-internet-of-things-has-a-language-problem.

3. Valhouli, Constantine. "The Internet of Things: Networked Objects and Smart Devices." The HammerSmith Group 2010. Accessed December 1, 2014. http://thehammersmithgroup.com/images/reports/networked_objects.pdf.

4. Neal, Meghan. "Researchers Say the Internet of Things Could Piggyback on Existing Networks." Motherboard. August 14, 2013. Accessed December 2, 2014. http://motherboard.vice.com/blog/researchers-say-the-internet-of-things-could-piggyback-on-existing-networks.

Melanson, Donald. "The Internet of Things Is One Step Closer to Being Powered by Wifi." Motherboard. August 6, 2014. Accessed December 2, 2014. http://motherboard.vice.com/read/the-internet-of-things-is-one-step-closer-to-being-powered-by-wifi?

Cox, Joseph. "The Internet of Things Can't Keep Your Data Safe." Motherboard. July 31, 2014. Accessed December 2, 2014. http://motherboard.vice.com/read/the-internet-of-things-has-your-personal-info.

5. Evans, Benjamin. Interview by author. April 1, 2015.

6. Rockwell, Mark. "Why FISMA Is Not Enough for the Internet of Things -- Federal Computer Week." August 1, 2014. Accessed April 2, 2015. http://fcw.com/Articles/2014/08/15/IoT-security-concerns.aspx?utm_source=The Pulse 8-18&utm_campaign=The Pulse 8-18&utm_medium=email&Page=2&m=1.

7. "Technological Advisory Council." Lecture, from FCC, Washington, D.C., December 4, 2014.

8. Giancarlo, Fortino, Anna Rovella, Wilma Russo, and Claudio Savaglio. "On the Classification of Cyberphysical Smart Objects in the Internet of Things." Central Europe (CEUR) Workshop Proceedings. May 27, 2014. Accessed January 10, 2015. http://ceur-ws.org/Vol-1156/paper7.pdf.

9. Koizumi, Kei. "Investing in America's Future through R&D, Innovation, and STEM Education: The President's FY 2016 Budget." The White House. February 2, 2015. Accessed April 4, 2015. https://www.whitehouse.gov/blog/2015/02/02/investing-america-s-future-through-rd-innovation-and-stem-education-president-s-fy-2.

10. "Federal Trade Commission Staff Report On the November 2013 Workshop Entitled The Internet of Things: Privacy and Security in a Connected World." Federal Trade Commission Staff Report On the November 2013 Workshop Entitled The Internet of Things: Privacy and Security in a Connected World. January 1, 2015. Accessed March 29, 2015. https://www.ftc.gov/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things.

11. *DHS IT Duplication Reduction Act of 2015* House of Representatives. Hurd §1626 (2015).

12. "Workshops." Federal Communications Commission. March 14, 2015. Accessed April 4, 2015. http://www.fcc.gov/workshops.

13. "Special Access Data Collection -- Glossary of Terms." Federal Communications Commission. March 14, 2015. Accessed April 4, 2015. http://www.fcc.gov/encyclopedia/mandatory-data-collection-glossary-terms.

14. Adler, Richard. "The Net: From Cyberspace to Everyplace." Computerworld. September 16, 2014. Accessed September 25, 2014.

Appendix A

Analysis process conducted

Steps for completion:

- **Topic decision**
- **Background research**
- **Project proposal**
    - Research methods proposal
    - Current understanding assessment
- **Hypothesis development**
    - Developed several mutually exclusive hypotheses about how the IoT can be implemented into the Federal Workforce over the next 20 years
    - We did hypothesis comparison, and we supported the hypothesis that we felt was the most plausible based upon the evidence we had gathered.
    - Below are listed hypotheses that were tested for potential expansion in the analysis. First hypotheses were generated after a level of context was established. After supporting or rejecting the hypotheses they later became expanded into scenarios of causal factors of the IoT expansion into the federal workforce.

Hypotheses

1. If government policy on IOT does not coincide with standard practice for private sector communication, there may be a distinct technological disadvantage resulting in slower IOT acceptance in the federal workforce which may ultimately cause the theft of intellectual property.

a. Deniable distance- limiting access to technology
b. Economic espionage/sabotage

2. If the US government does not establish security requirements for IOT technologies, then the number of unsecure nodes that attackers could hijack to infiltrate the federal network, could exponentially increase consequently exposing valuable government assets and information to cyber espionage, electronic sabotage, fraud, and theft.

3. If government systems compartmentalize the growth of IOT into local intranet type models, the resulting security benefits may outweigh a larger and more vulnerable wide area network while not sacrificing too much convenience.

4. If the government over the next 20 years begins to influence the private sector in the production of IOT technologies in order to accommodate the security requirements they deem necessary, then the federal workforce could successfully implement the IOT without sacrificing convenience and security in a globally competitive market.

a. Note: If the federal government influences the production of the products from their birth then they won't be stuck with the problem of recognizing a device and then saying "how do we secure it?" because the private sector manufacturers will develop products around the preemptively established security requirements.

- **Determine best evidence for**
    - It is important to note that this stage in our analysis was conducted alongside our hypothesis generation and testing.
    - We continued to conduct research in order to gain contextual information throughout this stage in our analysis. We sifted through this information to gain evidence and refuting information for all of our hypotheses and used the refuting evidence to lead us to the rejection of hypotheses and backing of our supported hypothesis.
- **Determine backed hypothesis – one we chose (eliminate others)**
    - After comparing the hypotheses alongside the evidence for and against the hypotheses we chose to back the hypothesis we did after wordsmithing it a bit to mitigate some of the refuting evidence.
- **Threat assessment of the IoT being implement into the Federal Workforce**
    - We examined the historical behavior of hackers
    - The broad intent of attackers historically and currently
    - Most likely targets
    - Means of attacking those targets
    - Most likely strategy of attackers
    - Then we assessed if each one of these elements would remain the same of change with the implementation of the IoT
- **Quadrant analysis of more specific scenarios that could develop under the umbrella of our hypotheses as a result of the driving factors that we chose.**
    - We used the drivers: Government influence on the design of IoT products and Security concerns (public's/government's interest in security) in a globally competitive market to be the causal factors of our scenarios.
    - These driving forces are (what we believe) to be the two driving forces that will more significantly play a role in shaping the development and integration of the IoT into the federal workforce.
- **Counterfactual reasoning to identify uncommon scenarios (the outliers)that might not have been thought of at this point, identify intermediate states that**

will occur as the scenario over the next 20 years develops, and identify triggers for the scenarios.

- Our counterfactual scenario is that the United States would fall behind in the IoT development, and that they would no longer be a frontrunner in IoT development.
- The trigger for this scenario is that their are major pushbacks from the Federal Government and/or the public about the IoT integration into the Federal Workforce.
    - Pushbacks does not mean regulation rather resistance against the implementation of these technologies vs. allowing their implementation and developing strategies to mitigate their risks
    - These pushbacks would allow foreign competitors facing less pushbacks to climb above American companies in IoT development
- The implications of this scenario would be that the U.S government would then have to determine a way to regulate the security of IoT devices that are being developed outside of the United States by foreign companies, an area outside of their span of control.

- Conclusion – includes (implications and recommendations)
    - We discussed the many implications of our findings for our consumer
- BLUF development
    - Upon completing our analysis we were then able to develop our BLUF to be short, concise, and encompassing of everything that we addressed with our analysis.

Appendix B

Context

IoT Technology represents an emerging market of devices that feeds into big data. Companies are connecting everyday devices to the internet in order to provide more convenience to the customer. For example, a customer can adjust the temperature of their house remotely if they have a "smart" thermostat that is connected to the internet. Due to the fact that this technology provides more convenience to users, it without a doubt continue to develop and integrate into everyday life. While these "smart" devices are exciting for users, they pose threats to the networks they are connected to, for they are unsecured gateways into the network. This creates a problem as the IoT is integrated into the federal workforce and when these devices begin to connect to the government's networks because attackers trying to access the government's big data will have easier entrances into the network. Currently, there are virtually no government regulations dictating the security requirements or capability restrictions that these devices may need, thus leaving the growing number of nodes on the federal network unsecured and open for penetration by hackers. Currently, no federal law comprehensively governs privacy and security of personal information in regards to IoT technologies, though several government organizations have begun to assess the need for some regulation.[10] In November of 2013, the Federal Trade Commission discussed the security concerns but ultimately did not develop any plan for regulation.[10]

The data becoming available via the use IoT technologies is expanding at an exponential rate to both the public and private sector. CISCO expects 400 zettabytes of information (400 billion terabytes, over 10 TB per human on the planet) to have been recorded by 2020[14]. The data that IoT devices are collecting for government application has implications for effectively managing public works, roads, infrastructure, worker efficiency, city planning, rail systems, etc. Through hardware instrumentation connected to the IoT, nearly every manageable resource can provide unique information to aid in governance but also presents avenues of approach for attackers leaving critical infrastructure and big data at risk. Imagine a cyber attacker wishing to do damage to the United States' critical infrastructure connecting to an IoT device that has a function within the power grid. An attacker could do catastrophic damage, collect an incredible amount of intelligence, or use these devices as gateways to deeper information stored in the government's big data.

With a high level of security concerns in a globally competitive market and a high government influence on products, the resulting environment is one where their there is high security requirements for IoT technologies leading to a global adoption of IoT technology. Global investment of the technology may continue to rise as implementation in both public and private sectors in the United States rises. Security protocol of hardware

is well established and enforced as data collection becomes nearly ubiquitous. Big data collection has risen to 400 zettabytes (400 billion terabytes) and far exceeds the amount of information any organization can reasonably process.[14] Data consumers of all kinds focus on collecting more timely, relevant data for decision making. Foreign adversaries may not remain a threat in the global competitive market or continue to conduct sophisticated and targeted attacks without developing new strategies to navigate around the security protocols established.

As the federal workforce implements the IoT it is important that the decision makers know the difference between critical, non critical systems, and infrastructure systems because for each of these categories of devices, there are different amounts of acceptable assumed risk. Providing the environmentals to a site or a network are the infrastructure systems, and these may include devices that have to do with space, power, or cooling. Smart racks/cabinets that house servers, switches, storage arrays, etc. are the infrastructure IoT devices that provide the space for the devices that house big data. Smart power distribution units (PDUs), static switches, uninterrupted power supplies (UPSs), and generators all provide power for the devices holding data, and are key infrastructure that are now vulnerable to the IoT. Lastly, smart remote controllers on chiller towers that cool data centers where big data is stored, smart thermostats, and smart alarm systems are all parts of the infrastructure that is now implementing the IoT technologies. Other devices that could be included under the umbrella of infrastructure may be lighting systems, camera systems, security systems, etc. All of these devices, are implementing IoT technologies, consequently becoming vulnerable to cyber sabotage via the IoT vulnerabilities.

Additionally, there are non-critical and critical systems in any network. The non-critical systems are generally an exact replica of the critical systems in the network for redundancy purposes. The non-critical system is called a development environment that is generally used for new projects that have not been published and for data recovery purposes in the event of a failure. The implementation of the IoT would likely first occur in the non-critical environment first and then it would naturally move into the critical environment. Critical systems have less acceptable assumed risk than the non-critical systems.

An example of a reactionary policy that addresses developing security concerns is the U.S Army's establishment of a cyber branch. The increasing need for the cyber branch also gives rise to the growing influence that the US has over the policy concerning the production of the IoT technologies. With those technologies being produced faster than policy can be written, the branch also has the duty to help detect and prevent attacks on the federal system. Hand-in-hand with this protection comes the counterattack obligation to trace the threat back to the source and properly shut it down. Despite these

benefits provided by the Cyber branch, they come at a price that taxpayers are left to pay. It can be very expensive to train the soldiers needed to run the systems and man the monitoring stations. This coupled with the cost of the equipment and the programs needed to create the system and the cost of keeping these systems running all the time, can initially appear to be an overwhelming price. This is the epitome of a costly and reactionary policy in response to the growing security concerns brought about by the development and implementation of new technologies such as IoT devices. If the U.S government is going to develop a proactive strategy in defending against various security threats than, it could develop policies that influence the production of these devices. This may facilitate a drastic decrease in the number of unsecured IoT devices on the internet that could be used to threaten the government's big data or critical infrastructure.

Appendix C

Quad Chart

This represents several possible outcomes for changes in security concerns in the globally competitive market into the future compared to the US government's influence on IoT products. Figure 1 represents the whole chart, while 2, 3, and 4 represent expansions of the key concerns for each scenario.

fig 1.
Figure 1 illustrates four major potential scenarios that could develop as a result of major causal factors.

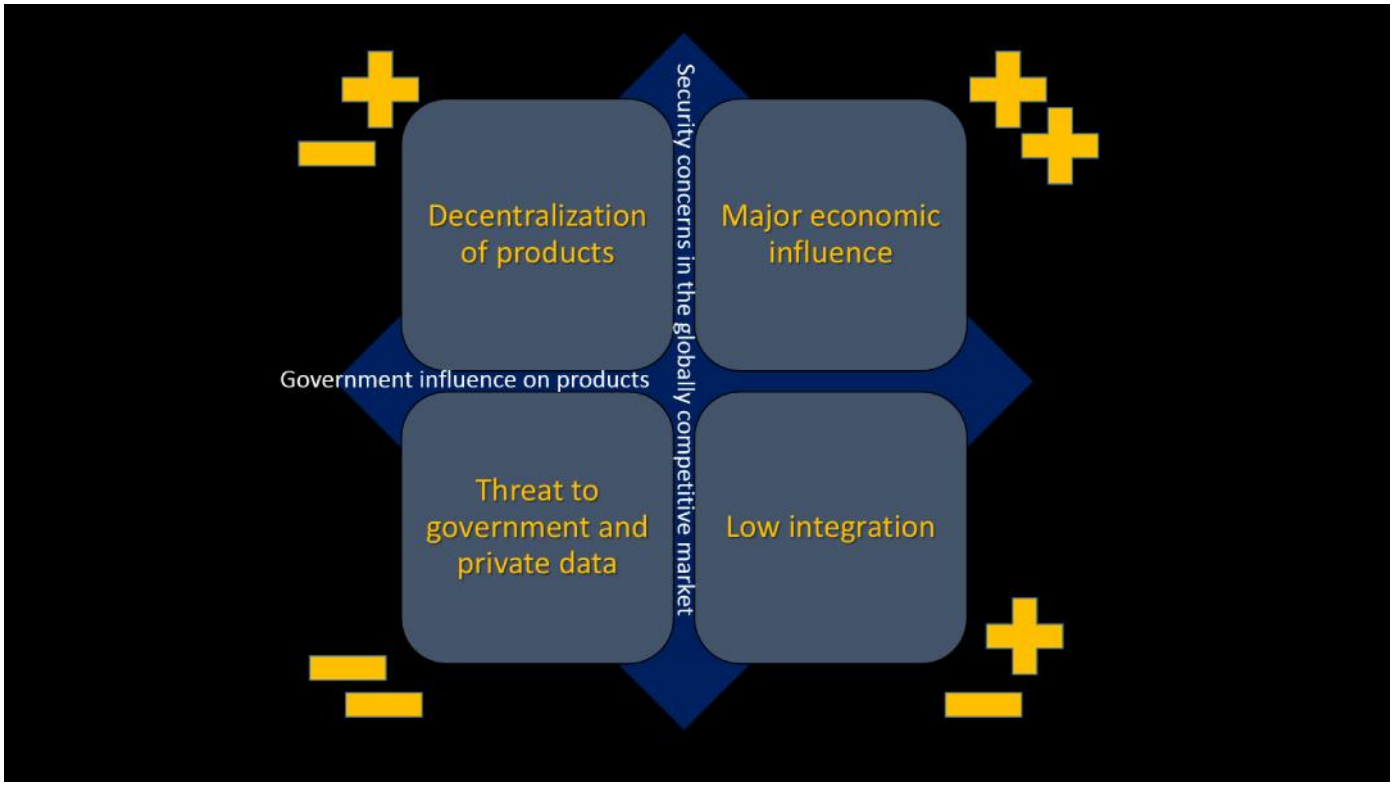


fig 2.
Figure 2 represents the top right scenario from the quad chart. With high spending and security, integration levels are high. These levels of support can be supported in r&d as well as a projection of policy needs. With an understanding of drivers and what this factors in this quadrant would look like, a counterfactual scenario can be developed. This is the most probable quadrant in the chart and leads to the counterfactual scenario.

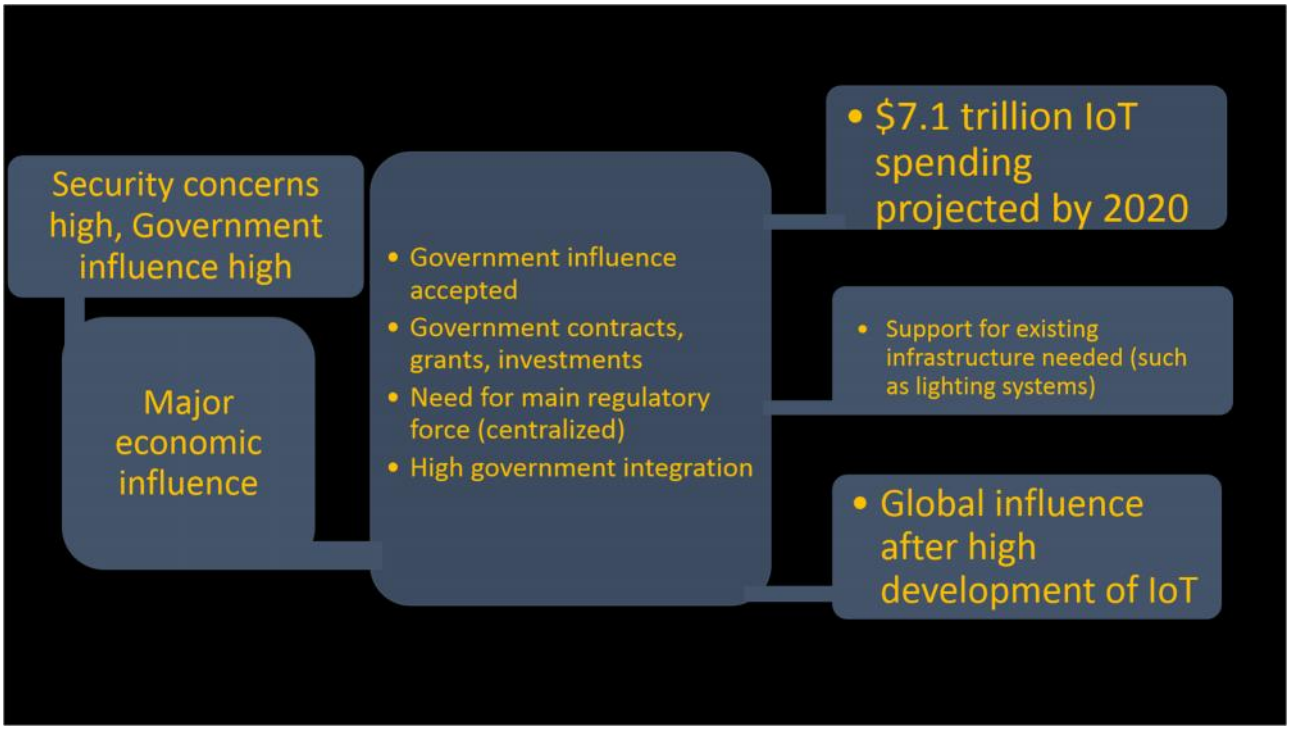


fig 3.

This is the second most probable scenario would result in a lower integration of IoT (in the near future). This would be caused by low security concerns and a high government influence. This scenario is supported by an understanding of the context of IoT, though this possibility could also lead to the counterfactual scenario.

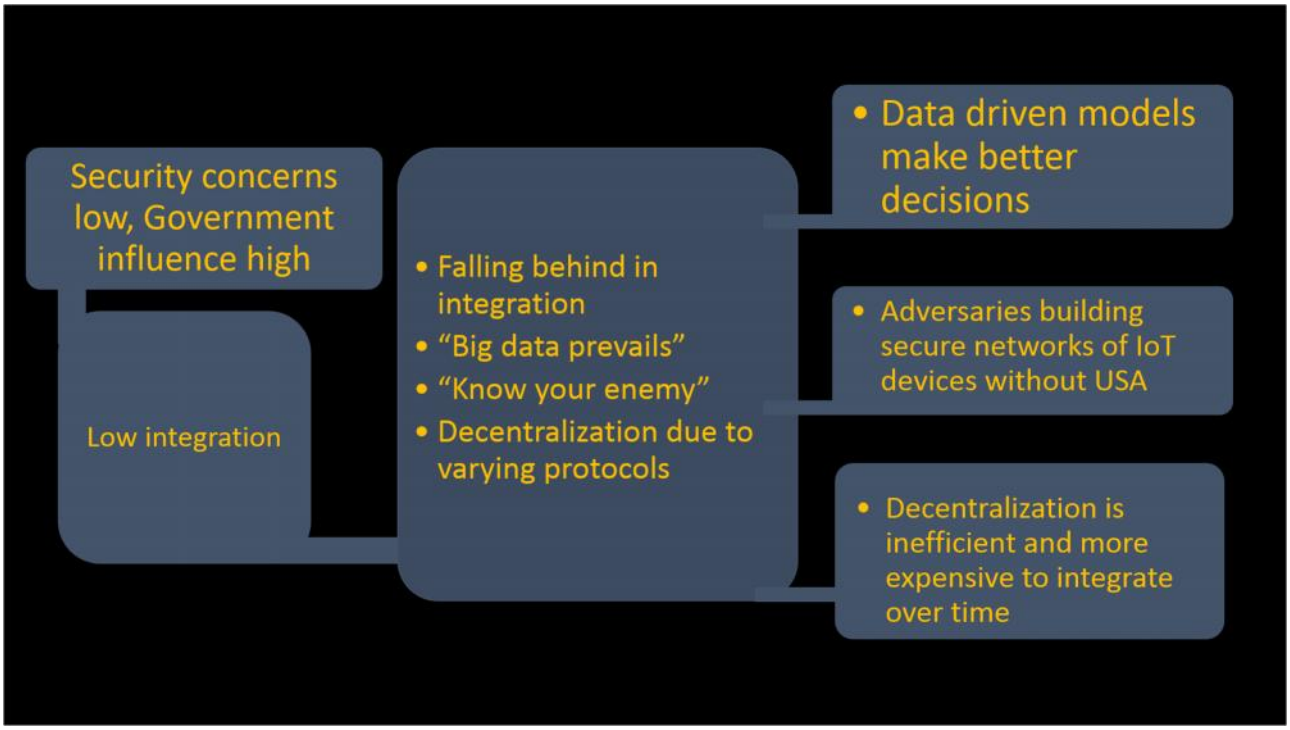
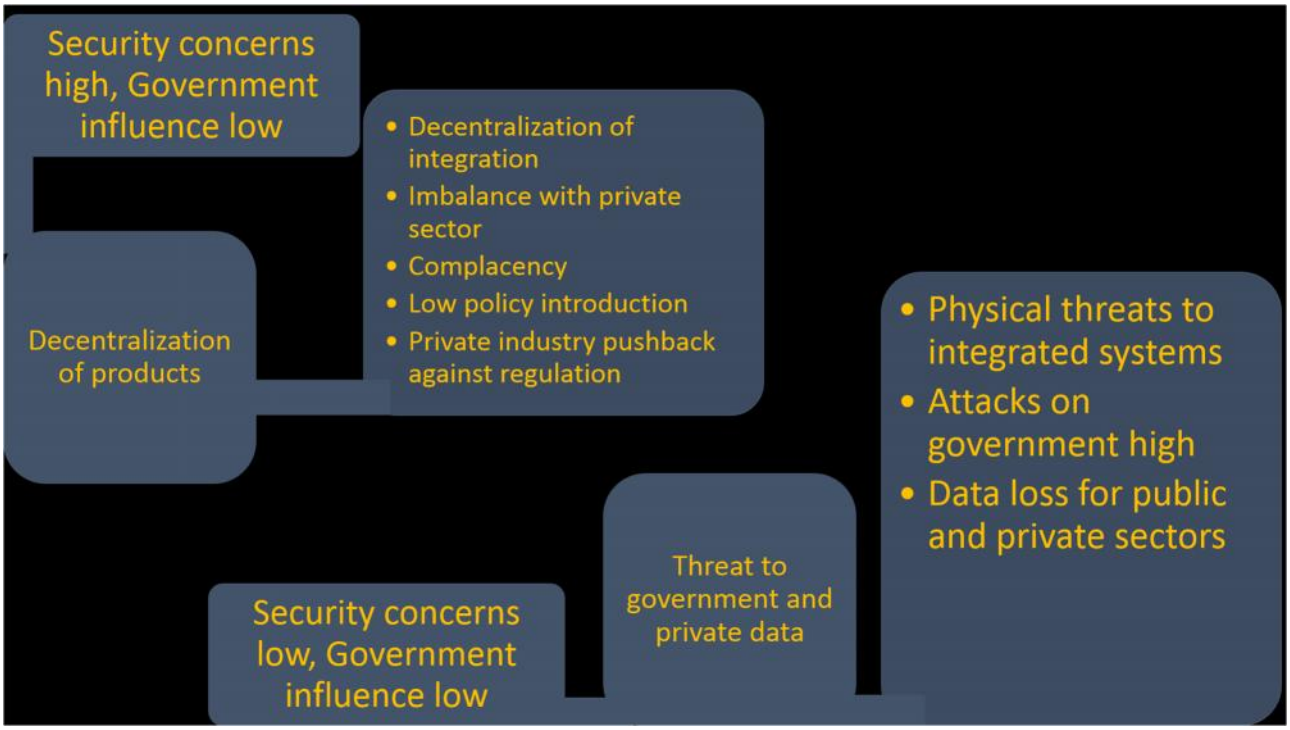


fig 4.

These two quadrants are the least probable. They do not support the inevitability of integration (eventually). They are still relevant to the decision making as any other reasons for low integration or threats to government data have potential triggers that can be assessed.


Security concerns high, Government influence low
• Decentralization of integration
• Imbalance with private sector
• Complacency
• Low policy introduction
• Private industry pushback against regulation
Decentralization of products
• Physical threats to integrated systems
• Attacks on government high
• Data loss for public and private sectors
Threat to government and private data
Security concerns low, Government influence low

Appendix F

8 Steps to successful integration

The IoT can be implemented in several structured steps to ensure security at each step and control of critical systems in order to maximize integration success. Audits between each step may identify weaknesses in systems. These steps may intermix as systems are phased in but would be monitored carefully to ensure security at all times. A failure in security will result in data loss ultimately causing rejection of acceptance of IoT in the government network. These steps are referenced on page 6.

Step 1: Authority (control point)
FCC

Step 2: Security protocols

Step 3: Universal standards through investment and policy

Step 4: Education to public and private sector

Step 5: Integration into infrastructure

Step 6: Integration into non critical systems

Step 7: Integration into critical systems

Step 8: FCC coalition with international regulatory systems such as ……(ex. OFCOM)