Federal IT Policy Recommendations: 2021-2024

Executive Summary

The work improving technology in government through policy initiatives over the last twelve years has been very successful, however there will always be more work that needs to be done. Today, there are several key steps that the Biden Administration could immediately address and work on over the next four years to continue to build trust and drive maturity in technology across government to “Build Back Better” — not just at the Federal level, but state and local as well. These steps include:

1. Renew the Commitment to Open Data & Transparency
2. Focus on Outcomes, not Box-Checking
3. Drive Customer Experience & Human-Centered Design
4. Solve Identity Once and for All
5. Increase Attention to Small Agencies and
6. Manage Risk through Security

I’ve spent the last ten years working on civic tech from local to Federal levels, inside and outside of government, and have been excited to see incredible gains in the government’s ability to deliver services to constituents. After the Obama Presidency, the work to drive innovation in government didn’t suddenly stop — the Trump Administration pursued an aggressive agenda of IT Modernization. This included a major effort to update a very large amount of outdated government technology guidance, laying the critical foundation for many modern technology practices and ideas.

From 2017–2019, I served in the Office of Management and Budget (OMB) in the Office of the Federal Chief Information Officer (OFCIO), where I worked on the new Federal Cloud Computing Strategy, ”Cloud Smart.” I designed this strategy to drive maturity across the Federal Government by updating a variety of older, interrelated policies on cybersecurity, procurement, and workforce training. At the time, we had no idea that many of these initiatives, such as the update to the Trusted Internet Connections policy (TIC), would be critical to enabling government-wide mission continuity during the COVID-19 response just a few months later.

From the past 4 years spent in government, I have been able to see many opportunities for improvements that did not get as much attention as they deserve. What follows are a few policy areas that I believe would build trust and improve service delivery to the American people. These aren’t all major innovations, but these efforts are needed to Move Carefully and Fix Things.

1. Renew the Commitment to Open Data & Transparency

Before joining the Federal Government, I spent years working for government transparency organizations including the Sunlight Foundation and the OpenGov Foundation. Although those and many other transparency organizations have shut their doors over the last four years, the need for transparency has never been greater.

However, I no longer hold the naive belief that sunlight is the best disinfectant. As it turns out, disinfectant is a better disinfectant, and regularly putting in the work to keep things clean in the first place is critically important. Transparency is an active process, not an end in and of itself — and **care will have to be given to rebuilding** some of the atrophied muscles within government.

Share Data on the Fight Against COVID-19

First and foremost, to heal the country a new Administration will need to deal with not only the COVID-19 virus, but also the *disinformation virus*. To do so effectively will require addressing public trust around information quality and availability. The Administration should **focus on providing timely, accurate information** including infection rates from Health and Human Services (HHS), job numbers from the Department of Labor (DOL), housing data from Housing and Urban Development (HUD), and loan data from the Small Business Administration (SBA). By **utilizing the new Chief Data Officers across government** installed as part of the Open, Public, Electronic and Necessary, (OPEN) Government Data Act signed into law in 2019, the Biden Administration would be able to gather and centralize the critical recovery data. Everyone loves shiny dashboards, but I would instead propose that **sharing raw data** to allow independent analysis would be vastly more valuable than Yet Another Dashboard.

Revise the National Action Plan

My work on the Fourth National Action Plan for Open Government (NAP4) — and the challenges the Trump Administration faced in delivering this plan — are matters of public record. As we look towards the Fifth National Action Plan, it will be critical to improve engagement with the public and open government groups. Since most of the country has quickly become accustomed to remote collaboration due to the pandemic, I would recommend **hosting a variety of virtual forums beyond the DC area** to maximize input and idea-generation outside of the beltway. In addition to bringing in more stakeholders from across the country, this would also aid in empowering grassroots-initiated activities towards anti-corruption practices as well.

I'd also recommend starting this process as early as possible to develop and gain traction around high-quality, ambitious commitments. There are also more than a few initiatives that civil society has proposed over the last decade that are worthy of reconsideration, including these from the NAP4.

Revise Agency Open Government Plans

As part of this work, OMB will need to update the long-neglected Agency Open Government Plans guidance, which has not been revised since 2016. Although most agencies have updated their Open Government plans since then, more ambitious efforts to publish data are needed. Notably, the Department of Veterans Affairs (VA) have not updated their plan since 2010, even though more scrutiny has been paid to them by Congress during this time. The VA Inspector General also previously identified that the VA had been actively working to undermine efforts to measure their progress on improving patient wait times, as a result of simply not recording data on the topic. With the new, $5 billion Electronic Health Records (EHR) system being implemented today, it is even more urgent that the VA improve their transparency.

However, **all Federal agencies should be directed to more aggressively and proactively publish data**, instead of just as a response to Freedom of Information Act (FOIA) requests. Throughout the Trump Administration, key datasets have been removed from government websites. The new Administration can both better tell its story and also build confidence in the American people using government services by **working to restore key data and increasing the volume of information that is actively shared**.

Rebuild The Office of Science and Technology Policy

The Office of Science and Technology Policy (OSTP), headed by the Federal Chief Technology Officer, was previously the center of open government work under the Obama Administration, but this office and its authority were dramatically reduced over the last four years, with staff cut from 150 to less than 50. As a result, **major reconstitution of OSTP and other offices will need to be done** to drive these efforts.

2. Focus on Outcomes, Not Box-Checking

Narrow Oversight Focus to High-Impact Projects

Transparency goes hand-in-hand with oversight. The Office of Management and Budget is the primary oversight organization within the Executive Branch (other than Inspectors General), and is organized into smaller domain-specific offices. Staff in these program offices act as "desk officers," focusing primarily on the 24 large CFO Act Agencies. For smaller offices, a single individual may be tasked with oversight of several agencies' billion dollar budgets. OMB's OFCIO is one such smaller office that has been stretched thin in this oversight duty while having to simultaneously fulfill a variety of policymaking roles. However, the primary role of this office is to oversee technology implementation across government to ensure the success of projects.

Given the few remaining staff, rather than being stretched thin on meaningless compliance, these resources could be better spent primarily focusing on only the **top five or ten major technology projects in government and making sure that they do not fail** in the way we saw happen with Healthcare.gov. Projects such as the State Department's passport & visa modernization, the Department of Veterans Affairs new EHR system, and other similar initiatives could greatly benefit from closer scrutiny. By investing in hiring subject matter experts with skills in technology and managing massive projects, the government could save taxpayers billions of dollars while simultaneously improving services. OFCIO should also collaborate closely with the Office of Performance and Personnel Management (OPPM) which oversees the Customer Experience initiative across government to make sure that these projects also meet the needs of the American people.

Restore and Expand The Office of the Federal Chief Information Officer

Moreover, OFCIO shares its limited budget with the U.S. Digital Service's (USDS) core operations via the Information Technology Oversight and Reform (ITOR) Fund, which was slashed dramatically under the Trump Administration. More than just paying for staff salaries, this fund is used to fund a variety of key technology oversight projects, such as the government's software code sharing initiative, code.gov. Cuts to this fund have caused OFCIO to eliminate programs like pulse.cio.gov, which monitored and evaluated the maturity and security of agency websites. Moreover, this fund is *flexible* and can be used by OMB to fund interesting technology initiatives at other agencies. The new Administration should **restore the ITOR budget**. It would also be useful to further supplement this fund by taking the step of working with Congress to set **appropriations to ensure the future of OFCIO and USDS**.

Like OSTP, OFCIO has experienced large setbacks. The constant budget cuts and toxic culture have decimated the office, and most of the talented & passionate subject matter experts I served with have since left. Reversing the course on this office, and **investing in hiring experts** with practical experience in *technology in government* — not just Silicon Valley thought leadership solutionism — in these offices and beyond will be critical for the success of Federal IT for the next four years. This will improve both the quality of policy that is created as well as the outcomes of IT projects governmentwide.

3. Drive Customer Experience & Human-Centered Design

Historically the government spends hundreds of millions of dollars on major IT projects. However, very little work is typically done to make sure that the right thing is being built — or if the right problem is even being solved. And sadly, newer systems are not always better systems. However, initiatives on Human-Centered Design (HCD) — a process to engage service recipients as stakeholders in the design and implementation of those services and systems — that were started under the Obama administration were built upon over the last four years. For instance, common private sector practices like user research and testing were previously considered difficult in government because of review & approval requirements under the Paperwork Reduction Act, but using streamlined processes and blanket-permission requests these barriers have largely been eliminated for most agencies. **These efforts need continued attention and support to maintain the momentum.**

Drive Commitment to Human-Centered Design Across OMB

At OMB, the Office of Information and Regulatory Affairs and the Performance & Personnel Management office worked to institutionalize much of this work over the last four years, including new governmentwide Customer Experience (CX) metrics guidance and a related Cross-Agency Priority Goal as part of the President's Management Agenda. These metrics should be considered table stakes for driving customer experience, and much more work must be done in this area. For instance, every major (and possibly even minor!) **IT project should have CX metrics defined as part of its requirements**, and these should be tracked throughout the life of the project. For existing projects, these should be created retroactively — starting with the highest-impact public-serving systems — with adequate baselines so that agencies don't just receive an "easy A." The recent General Services Administration (GSA) Playbook on CX may provide a great starting point for most agencies.

Fix the Definition of Agile

Of course, this customer experience work is not a new idea — in fact, this sort of Human-Centered Design is a core tenet of Agile software development. Unfortunately, the Federal Government has completely missed the forest for the trees on the principles of Agile, and almost all law and regulation focuses entirely on one area: incremental development, delivering software in small, working chunks over time, instead of delivering a full solution at the end of a lengthy development process. However, the real value of Agile is not in these small chunks, but rather in regular testing – both automated as well as having **actual members of the public using the service directly involved in the development process** to give feedback as the project progresses. In this way, teams can make sure their software works and is actually solving problems for people using the service, instead of *assuming* what the people served want. In the private sector we joke that you'll have testing either way — would you rather do it before your product launches when you can get ahead of the issues, or after when it's a public embarrassment?

Currently, agencies are required to report on their major IT investments and state if these projects are developed "incrementally," defined in guidance at the depressingly-low rate of once every six months. **OMB could refine their guidance to add additional Agile characteristics, including the requirement that software is tested throughout the development process with real customers.** This alone would dramatically decrease the number of failed projects in government, saving potentially billions of dollars.

Fund Great Customer Experience

However, all of this work requires expertise to be done well, and expertise comes at a cost. Champions such as Matt Lira have called for the creation of Chief Customer Experience Officers (CXOs) within agencies, which would be an excellent next step. However, we must not repeat the mistake of the creation of the Chief Data Officer (CDO) roles, where additional funding was not dedicated for these new roles or their staff – as a result this became yet another hat for the CIO to wear at most agencies. **Agencies will need to have increased funding in the President's Budget to both hire new CX experts as well as to fund contracts to support these efforts CX efforts government-wide.**

4. Solve Identity Once and for All

Accurately verifying a person's identity to satisfy Federal requirements, as well as creating a secure environment to allow them to login to Federal websites & tools, is a difficult and expensive task for all agencies. This also remains one of the biggest challenges for both agencies and the people accessing government services today. Most agencies have multiple login systems, each specifically tied to an individual service and without sharing information. For instance at the Department of Veterans Affairs until very recently there were nearly a dozen different login systems. Each of these systems would require you to prove that you are who you say you are separately as well.

Mandate Login.gov

Meanwhile, the GSA's Login.gov is an easy solution to this problem, and has been an overwhelming success for many agency services, including USAJobs, the website for most Federal job postings and application processes. Login.gov provides a simple solution to the very expensive problem of checking the identity of a member of the public and allowing them to login to a government website or application — to receive government benefits, register their small business, or any number of other services. This identity-proofing step is typically the most expensive part of the process, requiring the use of independent, private data sources like those used by our national credit bureaus. With Login.gov, once you're verified on one site you're verified at them all, so the cost for taxpayers is *dramatically* reduced.

Although some agencies are starting to move to this platform, a new administration should **mandate all agencies must use Login.gov**, and require them to **provide a transition plan to this service within 5 years**. In fact, usage of Login.gov is **already required by law**, but the law is simply not being followed (6 U.S.C. 1523(b)(1)(D)). Instead of just an **unfunded mandate,** the President's Budget should include a request for Congress to provide appropriations directly to GSA to fund these efforts to ensure this product is sustainable well into the future.

Use USPS for In-Person Identity Proofing

At the VA we also learned that many people have trouble with identity proofing over the internet for a number of reasons, including problems with having suitable cameras for capturing information from IDs, issues with people's memory that preclude standard address verification methods, and other issues. However, we found that people were much more likely to be successful by having their identity validated by humans in-person at VA hospitals. The US Postal Service (USPS) has successfully piloted a service to check people's identity in-person at both USPS locations and at people's homes using their existing portable tablets used for mail delivery. **By working with Congress to help fund this service**, identity verification could be a solved problem, while also providing a sustainable additional revenue stream for the desperately-underfunded USPS.

Share these Services with State & Local Governments

Moreover, **these services should be offered to state and local governments**, who are incredibly eager for these solutions, coupled with the expertise of the Federal government. For instance, the same login that you use for USAJobs could be used to login to your local DMV, once again making government easier and friendlier for everyone. To date, GSA leadership has not actively allowed sales to these governments, even though it is *explicitly allowed under law* and other similar services have been allowed, such as Cloud.gov. The White House should direct **GSA to provide this service to any government agency who wants it — and even to the private sector where appropriate!**

Recent bills in Congress have also prioritized security for state and local governments, so it would not be unreasonable to go even further and **work with Congress to set appropriations to provide this identity service** to them as well. Working closely with the Cybersecurity and Infrastructure Security Agency (CISA), GSA could turn this from a small project into a national program.

5. Increase Attention to Small Agencies

There are nearly a hundred smaller independent agencies that are not situated under the President's Cabinet, and as a result they are largely ignored. However, they still have critically important missions, and these agencies also interface with the bigger agencies to exchange data, presenting a number of potential security concerns and operational risks. Although a focus on projects and outcomes — not just compliance — is critical, OMB needs to pay more attention to these smaller agencies.

For instance, the U.S. Securities and Exchange Commission is a small independent agency of only 4000 people, but is tasked with protecting investors and the national banking system, as a result of the stock market crash in the 1920s. As such a small agency, they don't have nearly the budget for IT and cybersecurity of the large agencies. However, since they exchange data with the Department of the Treasury, they act as a backdoor into the larger agency. This sort of attack, by exploiting a softer target to gain access to a more secure one, is extremely common on the smaller scale and will inevitably become a focus for hostile nation-states in the future.

Fund Small Agencies' IT

These smaller agencies will need additional resources to be able to deal with these threats while also keeping their services up-to-date. OMB can take the much-needed step of **requesting larger IT budgets for these agencies.** Furthermore, to date no small agencies have been selected for Technology Modernization Funds — a "loan program" for agencies to fund IT projects — to help them improve their IT. Meanwhile massive organizations such as U.S. Customs and Border Protection (CBP) — who have an annual budget of *17 billion dollars* and are not in any way short of money — have received an *additional* 15 million dollars from this fund to update their legacy financial systems. Providing access to further funds for smaller agencies would give them an opportunity to improve their systems.

Drive Shared Service Use

Shared IT services are even more important for these agencies as well. In many cases the Chief Information Officer (CIO) will wear many hats — acting as Chief Information Security Officer (CISO), Chief Data Officer (CDO), and other roles. To be successful while being stretched so thin means that staff must take advantage of the capabilities of the bigger agencies to help them fill their gaps, such as the Department of Justice's Security Operations Center-as-a-Service offering. The idea of a "CIO in a Box" for the smaller agencies has been brought up several times, providing information, services, and resources to these organizations. However, very little movement has been made on this initiative and this is **a large opportunity for further work and investment.**

Other shared services, including the aforementioned Login.gov and Cloud.gov also would provide major benefits to smaller agencies, especially if the **President's budget included additional dedicated funding to GSA for these projects for small agencies**, so that they don't have to scrape together the money out of their own limited budgets.

6. Manage Risk through Security

The common theme here is that cybersecurity remains one of the greatest challenges for technology in government today. The Federal Information Security Management Act (FISMA) sets many of the legal requirements for cybersecurity in government, and in practice this has transformed risk management into *risk avoidance*, reducing the overall risk tolerance for agencies and freezing any interest in trying new things. There is little hope of Congress fixing FISMA in the near future, and the attempts to date only will make things worse. In the meantime, **the Biden Administration could supplement ongoing initiatives for security automation with additional resources, and implement the resulting best practices as official policy governmentwide.**

Continuous Security Authorization of IT Systems

At the center of IT security in government is the Authorization to Operate (ATO) process. If you've ever worked for the government, I'm sure you groaned just having to read that phrase. FISMA requires that for all IT systems, agencies must implement a series of "security controls" — measures defined by the National Institute of Standards and Technology (NIST) to enhance security. Now, this is an extremely laborious process, and a new product may take months to meet the requirements of a security review. This process generates a lot of paperwork — enough to stop bullets, but this isn't very effective for keeping out nefarious attackers. Many agencies only have a three-year cycle of re-assessing products for these security controls — basically only checking to see if the door is locked once every few years. Moreover, the interpretation and implementation of these controls differ wildly between agencies.

Several agencies have started separate pilots to improve the consistency and speed of this process. For instance, some agencies are working to implement a "lightweight authorization to operate" (LATO) or a "progressive authorization to operate" process where only a subset of the security controls must be reviewed to begin *developing* on a platform, with further controls added along the way before launching the application for public use. Others are moving to "continuous authorization," a concept similar to *continuous integration* for software testing, by using standard tools to automatically check the various security controls on an ongoing basis — providing real-time visibility to the security of the systems. Still other agencies are working to standardize security plan language, or use natural language processing (NLP) as a means of reviewing paperwork-heavy controls faster. These efforts also relate to NIST’s efforts to standardize controls via a machine-readable structure called OSCAL, which is now being used by GSA’s FedRAMP program. Some of these efforts were previously being replicated via the CIO Council, but with the exodus of OFCIO staff efforts have stalled out. These efforts should be **spread across government via additional funding, staffing, and more pilots**.

Conclusion

These are just a few of the policy areas that need attention in technology in government. There are still other agency-specific projects that need further attention that I haven’t covered here. However, these specific areas of focus will continue to build back better technology in government, and equip us with the necessary tools for the next decade or two.

Reskilling and Hiring in Government IT

The nature of business is **change** — we move, refine, and combine goods and services and data, which generates *value* — and this is true both in the public and the private sector. Technology is just one of the ways that we *manage* that change. Those organizations that do best at managing change are often the best equipped to deal with the relentless pace of transformation within the IT field itself. Government, however, tends to resist change because of misaligned value incentives which prioritize *stability* and avoid *risk*, though these elements do not necessarily need to be at odds with one another.

Since the Reagan era, government agencies have outsourced more and more IT tasks to contractors and vendors, under the false promise of reduced risk and increased savings for taxpayers. There's an infamous joke that we've done such a good job of saving money through IT over the last decade that we've reduced the IT budget of $2 billion to $40 billion. Yet almost all of that spending has gone to private companies, instead of increasing Federal staff and providing needed training, and the government has astonishingly little positive progress to show for it — systems and projects continue to fail. This effort has *lobotomized* government by eliminating subject matter experts, reducing its ability to manage change, and as a result has greatly increased — rather than reduced — the risk for Federal agencies.

Agencies have tried to "buy their way out" of their risk, by leveraging vendors and IT products to "absorb" the risk. Unfortunately, government doesn't work that way — agencies are solely responsible for risk, and if something fails, the agency, not the vendor, is the one on the hook for any lawsuits or Congressional hearings that result. **The only practical way for agencies to deal with their risk and begin paying down the government's massive technical debt is to hire and train experts inside of government who can address these problems directly, and begin to facilitate change management.**

In the Cloud Smart strategy OMB states, "to harness new capabilities and expand existing abilities to enable their mission and deliver services to the public faster … instead of 'buy before build', agencies will need to move to '**solve before buy**,' addressing their service needs, fundamental requirements, and gaps in processes and skillsets." Although there has been a major effort to hire and train cybersecurity professionals in government, technology literacy needs to be improved in all job roles. Technology will always be a core function of government, and to be successful, government *must* have expertise in its core functions; to do otherwise is to deliberately sabotage that success.

Efforts such as GSA's 18F Team and The US Digital Service (USDS) have proven that there is a need for this expertise, and the government must continue and expand on those efforts by teaching agencies "how to fish." Beyond just these short-term hires via Digital Service/Schedule A and Cybersecurity/2210 to augment staff temporarily,

agencies need to invest in *permanently* expanding their knowledge, skills, and capacity.

Increase Training Opportunities for Federal Government Employees

First, there needs to be a **governmentwide approach to increasing training**, starting with **additional funding in the President's budget dedicated to improving IT skills**. Financial and leave award incentives could also be used to encourage staff to participate in more training outside of their immediate job roles.

The Federal Cybersecurity Reskilling Academy as part of the Cloud Smart strategy was a good start, but didn't go far enough. It's impossible to fully train a practitioner in everything they need to know about Cybersecurity — or any other complex technology — in just a few short weeks. A real **apprenticeship program** in the form of agency rotation & detail programs for staff into more IT-mature agencies would have a major impact, by allowing staff to learn skills on-the-job in a hands-on way. Many of these skills are impossible to learn meaningfully from a book or seminar; in general most technical certifications — instead of being required — should be met with skepticism.

Almost all policy decisions today have some aspect of technology involved. To address the rapidly aging Federal IT infrastructure and make smart investments with taxpayer dollars, all of our leaders need to be equipped with knowledge of modern systems beyond just the sales pitches they receive from vendors. Ongoing training in technology must be made a priority and part of every Senior Executive Service (SES) performance plan.

Create a new IT Job Series

Although many technologists have been willing to work for a short term of 2–4 years in government at a massive pay cut just out of a feeling of civic duty, this sort of "holiday labor" is not a sustainable path for long-term success. A new Administration will need to **address the massive pay disparity for government IT jobs**, which acts as a barrier to both hiring and retaining staff. The White House will need to direct the Office of Personnel Management (OPM) to establish a proper IT job series or extend the 2210 CyberSecurity role definition, and create a special rate that reduces this gap particularly at the top end of the scale (GS-13 through GS-15).

Ideally this pay should be competitive with the private sector by locale, or as close to the standard rates as possible. And this pay must be made available to staff as they are retrained, *not just* to outsiders coming in to government with lucrative salaries from the private sector. Without this key step, the work done to reskill our staff will be lost as they use their new skills to find better-paying employment outside of government.

Also, this job series should include not only security personnel, software engineers, and graphic designers, but also non-traditional (but very important) members of government technical teams such as program & product managers, contracting officer representatives (CORs), customer experience experts, and content designers.

Leverage Modern Hiring Techniques to Bring in Skilled Personnel

Third, agencies must be directed to **aggressively move away from older hiring processes and switch to techniques which evaluate if candidates can actually do the job**. OPM, in coordination with USDS, has already done a lot of work towards this, including eliminating education requirements and moving to knowledge-based hiring techniques, but agencies largely have not yet implemented this new guidance. The White House will need to apply more pressure for these changes if agencies are expected to adopt them. Initiatives such as Launch Grad and the Civic Digital Fellowship could also provide a pipeline for potential candidates with critical skills into government service.

Improving Diversity in the Senior Executive Service

Finally, major improvements must be made to the Senior Executive Service (SES) hiring process. These staff represent the senior leaders at Federal agencies, and almost all policy decisions today have some aspect of technology involved. To address the rapidly aging Federal IT infrastructure and make smart investments with taxpayer dollars, all of our leaders need to be equipped with knowledge of modern systems beyond just the sales pitches they receive from vendors.

In addition to increasing critical technical knowledge of these key decision-makers, the lack of diversity of this group has gone woefully unaddressed even after years of critical reports. Since these SESs are on the boards that hire the other SESs, and many of these leadership roles are filled due to tacit political connections not the candidates' skills, it is unlikely that the diversity will improve organically from this in-group.

This entire hiring process needs to be reconsidered to level the playing field. The Executive Core Qualifications (ECQs) were a good idea to set a baseline for expertise in senior management, but have largely become an expensive gatekeeping exercise. This has given rise to a cottage industry of writers who simply churn out government resumes to a pricetag of *thousands* of dollars. I know of very few SES staff who were not either hand-picked for their first SES role or who paid to have their resume written by a professional. This limits these staff to those who can “pay to play” — either with literal dollars or political influence, severely limiting the candidate pool.

On the reviewer's end, it's long been known that overtaxed human resources staff are often just searching for keywords from the job postings in the resumes as a means of first review, which eliminates anyone who may have missed a *specific word or phrase*. Government expertise and education *appears* to be given a higher standing than outside experience as well. And after your ECQs have been approved once you don't need to have them re-reviewed for each job, further narrowing the list of candidates who are considered.

There is no single, easy solution to the systemic problems in this process. Expanding training opportunities for senior General Schedule employees (GS-14 and GS-15) beyond just the outdated and time-consuming Candidate Development Program would be a first step. A new Administration could make diversity a key priority in the President's Management Agenda, setting goals for hiring and new initiatives for recruiting under the Chief Human Capital Officers Council (CHCOC).

In Closing: Countering Bias Through Diversity

Our country is changing, and so is the nature of government. Diversity is critical for all technology roles in government, not just leadership. Addressing systemic bias in the tools that agencies are implementing will require attention from all levels of staff. Our benefit systems must provide services equitably to all, but this will be impossible without acknowledging these biases. However, due to a recent Executive Order, training around bias has largely been halted in the Federal government, reducing our ability to tackle this challenge. As the government begins to close gaps around technology skills, it is critical that we're building a workforce that reflects the people we serve, so that we can better address these issues at their root.

Principles for Automation in Government

Artificial Intelligence (AI), Machine Learning (ML), Robotic Processing Automation (RPA)[1], and other related predictive algorithm technologies continue to gain attention. However, at the moment their promises are far greater than the reality, and instead of successes we continue to see the worst of ourselves reflected back. Vendors also continue to oversell the functionality of these tools, while glossing over major expenses and difficulties, such as acquiring and tagging training data.

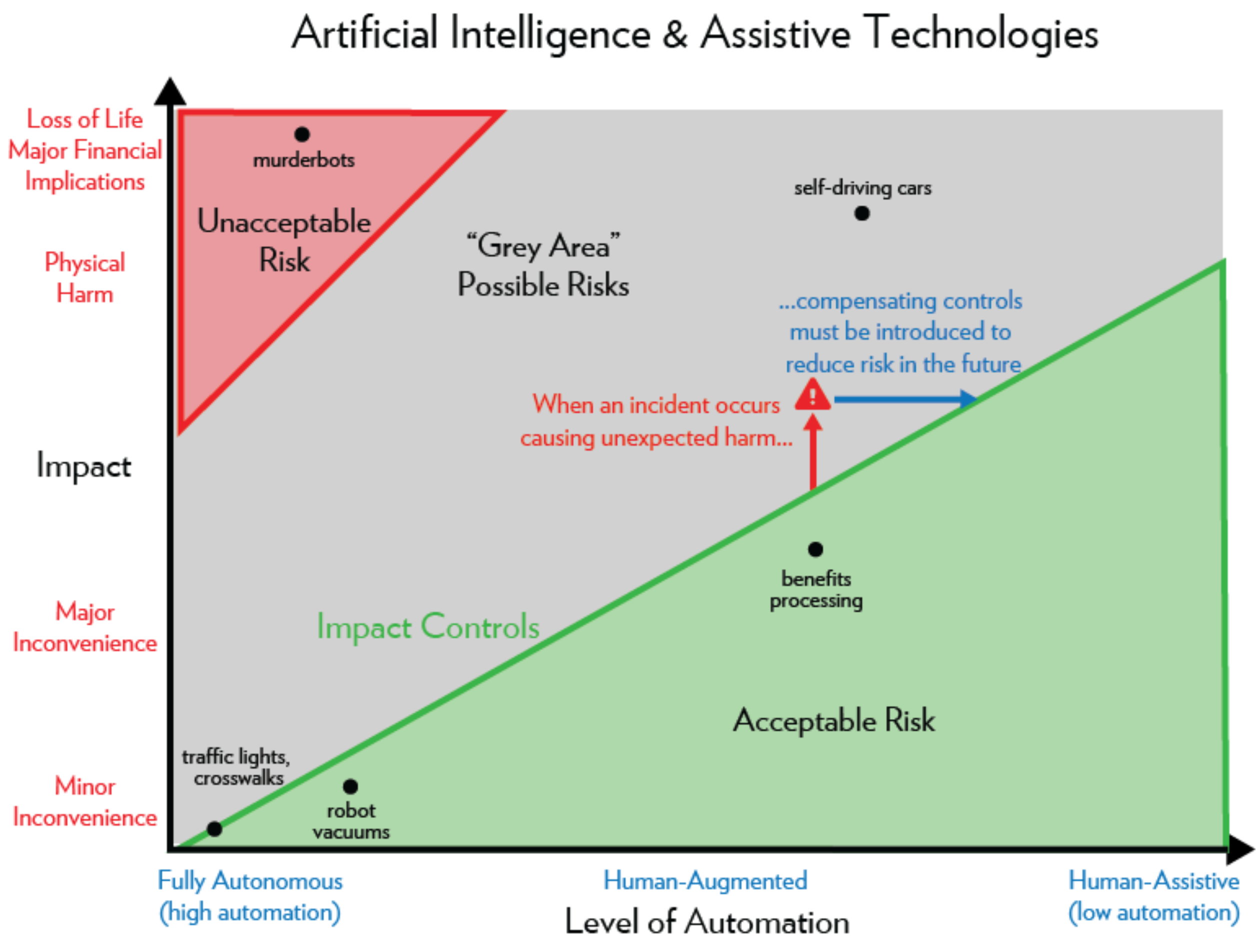
The Trump Administration, rather than increasing scrutiny and oversight of these technologies, only sought to reduce barriers to its usage. The Biden Administration will need to **create stronger protections for the American people through better governance of the usage of these solutions in government.**

The problem is that humans have written our biases into our processes, and automation only expedites and amplifies these biases. (The book Automating Inequality explains this better than I ever could.) As a technologist, I become concerned when I hear of government agencies implementing these technologies for decision-making, as our unequal systems will only lead to greater inequity. It's all too easy to "blame the algorithm" to avoid liability, but it's who humans create the algorithms.

Simply put, the Federal government cannot have racist chatbots. The government must not exacerbate the problem of minorities not receiving benefits they deserve. And the government should not be using tools that can reenforce existing racism and sexism while remaining willfully ignorant of these topics. Yet with all of these failures, we still see organizations running gleefully towards toxic ideas such as predictive policing and facial-recognition technology.

Fundamentally, **this is a question of ethics.** Although in government we have extensive ethics laws and regulations in regard to finances and influence, there is almost no actual guidance on ethical practices in the use of technology. And in the U.S. there exists no standard code of ethics for software engineering, no Hippocratic Oath for practicing technology. However, we do have a series of regulatory proxies for ethics, in the form of security and privacy requirements aimed to protect the *data* of the American people.

[1] Some of us technologists have referred to RPA as "Steampunkification" instead of IT modernization, as the older systems are still left in place while newer tech is just stuck on top, increasing rather than decreasing the technical debt of an organization— much as Steampunks glue shiny gears onto old hats as fashion.


Artificial Intelligence & Assistive Technologies
Loss of Life
Major Financial Implications
Physical Harm
Impact
Major Inconvenience
Minor Inconvenience
murderbots
Unacceptable Risk
"Grey Area" Possible Risks
self-driving cars
...compensating controls must be introduced to reduce risk in the future
When an incident occurs causing unexpected harm...
benefits processing
Impact Controls
Acceptable Risk
traffic lights, crosswalks
robot vacuums
Fully Autonomous (high automation)
Human-Augmented
Level of Automation
Human-Assistive (low automation)

A diagram reflecting the balance between human versus computer decision-making and impact to human life and livelihood.

By **requiring a series of controls**—not unlike those that we use for IT security—we can increase the safety of the usage of these tools. Similar to the current National Institute of Standards and Technology (NIST) classifications for Low, Medium, and High security systems, artificial intelligence systems should be classified by their impact to people, and the level of automation that is allowed must be guided by the impact. And like the NIST security controls, these must be auditable and testable, to make sure systems are functioning within the expected policy parameters.

For instance, a robot vacuum cleaner presents very little risk of life, but can cause some inconvenience if it misbehaves, so very few controls and human oversight would be required. But automation in the processing for loans or other benefits may disastrously impact people's finances, so higher controls must be implemented and more human engagement should be required.

Most notably among these controls must be **explainability in decision-making** by computers. When a decision is made by a machine—for instance, the denial of a benefit to a person—we must be able to see exactly *how and why* the decision was made and improve the system in the future. This is a requirement that megacorporations have long railed against due to the potential legal liabilities they may face in having to provide such documentation, but the Administration must not yield to these private interests at the expense of The People.

Another key control will be transparency in the usage of these systems, and all Federal agencies must be required to notify the people when such a system is in use. This should be done both through a Federal Records Notice similar to the ones required for new information systems, but also on the form, tool, or decision letter *itself* so that consumers are aware of how these tools are used. Standard, plain language descriptions should be created and used government-wide.

Related to that control, any system that makes a determination, on a benefit or similar, must have a process for the recipient to appeal the decision to an actual human in a timely fashion. This requirement is *deliberately* burdensome, as it will actively curtail many inappropriate uses in government, since overtaxed government processes won't be able to keep up with too many denied benefits. For instance, the Veterans Benefit Appeals system currently is entirely manual, but has a delay of a year or more, and some Veterans have been waiting years for appeals to be adjudicated; if a system is seeing an unreasonably large number of appeals of benefit denials, that's a good indicator of a broken system.

Moreover the result of that appeal must become part of the determining framework after re-adjudication, and any previous adjudications or pending appeals should be automatically reconsidered retroactively.

There also exists a category of uses of Artificial Intelligence that the government should entirely prohibit. The most extreme and obvious example is the creation of lethal robots for law enforcement or military usage—regardless of what benefits the Department of Defense and military vendors try to sell us. Although there's little fear of a science-fiction dystopia of self-aware murderbots, major ethical considerations must still be taken into account. If we cannot trust even human officers to act ethically under political duress, we certainly cannot expect robots devoid of any empathy to protect our citizens from tyranny when they can be turned against people with the push of a button.

Similarly, the government must also be able to hold private companies liable for their usage of these technologies both in government and the private sector as well. If something fails, the government legally owns the risk, but that does not mean that private companies should escape blame or penalties. The increase in companies creating self-driving cars will inevitably lead to more deaths, but these companies continue to avoid any responsibility. The National Highway Traffic Safety Administration's recommendations on autonomous vehicles do not go nearly far enough, merely making the "request that manufacturers and other entities *voluntarily* provide reports."

In short, the government must make a stand to protect its people, instead of merely serving the interests of private companies—it cannot do both.

Bill Hunt
hello@billhunt.email
https://billhunt.dev
Ph: 20-BILL-HUNT
(202 455-4868)