

Leading IT Transformation: Insights from Joe Klimavicz, Deputy Assistant Attorney General and Chief Information Officer, U.S. Department of Justice

By Michael J. Keegan




Today, more than ever, U.S. federal departments must ensure the security and reliability of their systems and information technology. In many ways, this also involves transforming how these departments deliver and consume information and technology

services. The U.S. Department of Justice (DOJ) is one of those many federal agencies working to modernize its IT infrastructure to meet the demands of today.


What are the key IT priorities of the U.S. Department of Justice? How is DOJ going from IT modernization to its transformation? Joe Klimavicz, Chief Information Officer, U.S. Department of Justice, joined me on *The Business of Government Hour* to share his insights on these topics and more. The following is an edited excerpt of our discussion, complemented with additional research.

What is the mission of your office? How is it organized and how do you support the overall mission of the U.S. Department of Justice?


 Before I talk about my specific office, I'd like to give a brief overview of the department. DOJ is a very broad and varied organization of over 40 components. Broadly, our high-level missions are to enforce the laws of the country; defend the interests of the United States according to the law; ensure public safety against threats, foreign and domestic; and prevent and control crime. As CIO, my mission is to provide high-quality and secure information and technology services that enable the mission of the department. The broad DOJ mission requires specific IT tools and services as well as shared enterprise IT. The office is comprised of four areas: service delivery, cybersecurity,

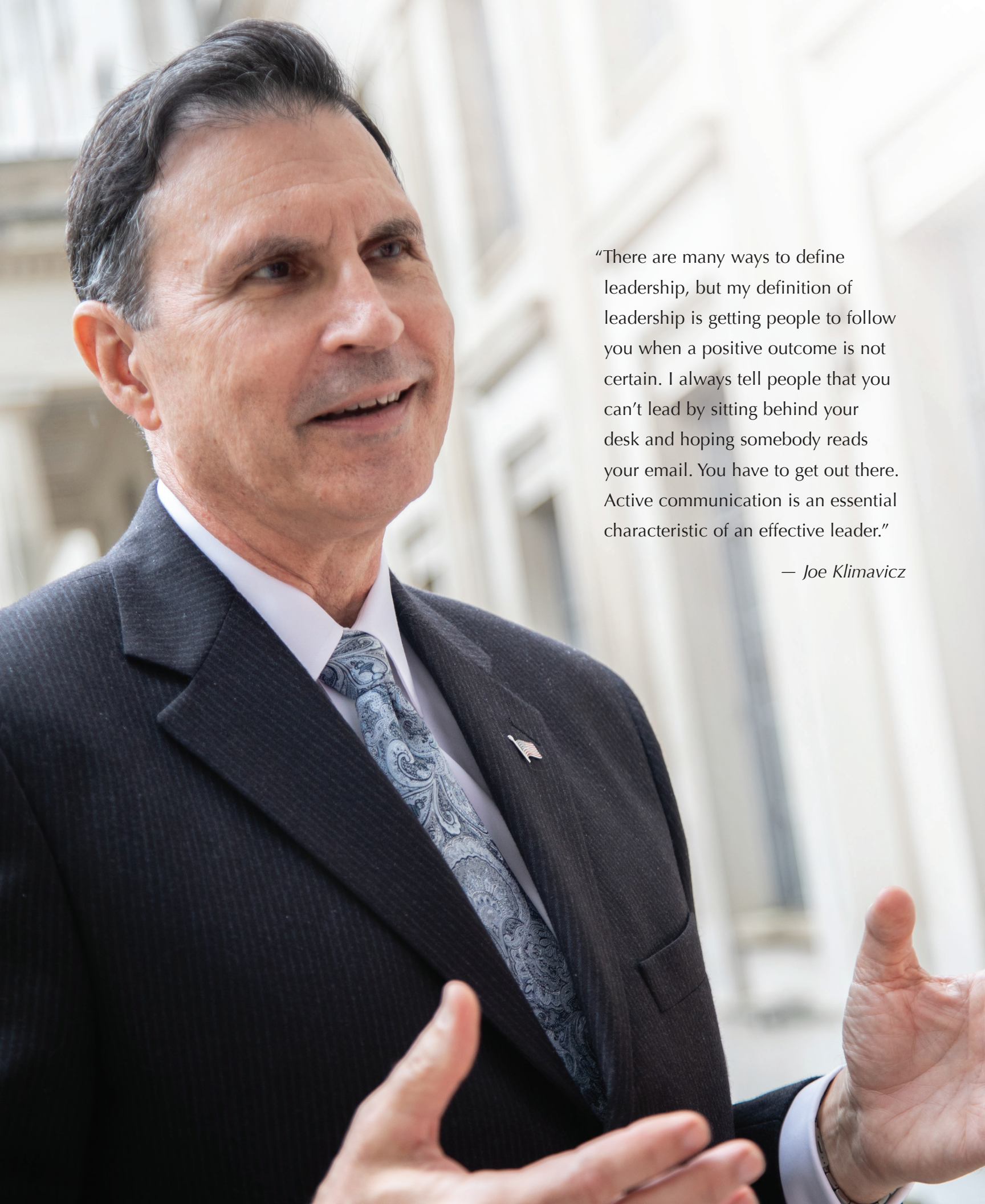
policy and planning, essentially our portfolio management, and service engineering staff.

What are your specific duties and responsibilities as the chief information officer?

 There are a couple areas. One is overseeing DOJ's IT resources, IT portfolio—and that's roughly about 10 percent of our overall budget, approximately \$3 billion annually. We need to make sure we're getting the value from that investment. I have to deliver IT services to the senior leadership, senior management offices, and provide enterprise services to DOJ. I have to protect DOJ's information and information systems from data loss or unauthorized access. I have to engineer, develop, and broker new enterprise IT services, and those can come from a lot of different places. I'm also the lead for all geospatial activities in the department, radio frequency, spectrum use, and interagency law enforcement information sharing.

What are your top three management challenges and how have you sought to address them?

 The three challenges are cybersecurity, modernization, and the IT workforce. Cybersecurity is probably the number one challenge. As everybody knows, cyberattacks are increasing in aggression, sophistication, and bypassing traditional security tools. I'm focused on enhancing and strengthening our security posture to defend against these attacks. We have very sensitive law enforcement, national security, operations, and missions. We're a target, so we have to help maintain the confidentiality, integrity, and availability of our systems.



“There are many ways to define leadership, but my definition of leadership is getting people to follow you when a positive outcome is not certain. I always tell people that you can’t lead by sitting behind your desk and hoping somebody reads your email. You have to get out there. Active communication is an essential characteristic of an effective leader.”

— Joe Klimavicz

The next challenge is modernization of our legacy systems. We've been really focused on that for a number of years. Legacy systems that are built with antiquated code contain inherent vulnerabilities and increase the attack surface. We want to make sure we are modernizing to not only to enhance our cyber posture, but also reduce our operating costs and enhance our general capabilities.

The last challenge is recruiting and retaining highly qualified IT personnel. We have to work within the federal hiring process, so you have hiring freezes and we have competitive pay issues as compared to the private sector. There are going to be difficulties in locating individuals with the right skills. The one area that we're really focusing on is training our existing workforce—making sure that they have access to the best training and doing everything possible to keep their skills current.

How do you lead? What are the characteristics of an effective leader?



There are many ways to define leadership, but my definition of leadership is getting people to follow you when a positive outcome is not certain. I always tell people that you can't lead by sitting behind your desk and hoping somebody reads your email. You have to get out there. Active communication is an essential characteristic of an effective leader.

You have to possess a laser focus on a consistent set of priorities. I always tell people that if you're not passionate about your job, go get another job because life is too short to waste on one that you're not really enthused about.

Leaders should choose their battles carefully. During the Revolutionary War, there were only nine major real battles. George Washington lost six of the nine, but he won the right three. It's important to figure out what's important to focus on rather than chasing everything. Additionally, you need to know yourself, your people, and your business. You need to convey a compelling vision and clear goals—priorities. Try to figure out how everybody fits into this and enlist everybody's help. Equip your staff to be able to get on board and support your goals. Act on facts and make decisions. I think too often we wait for perfect information to make decisions. Leaders must also demonstrate the highest standards of conduct, integrity, and professionalism. You're always on stage as a leader. Lastly, I would just say you've got to be a constant learner who isn't afraid of taking risks.

IT is critical to the success of executing DOJ's mission. Would you give us an overview of your strategic vision for IT at DOJ, and more particularly, what are your priorities?



My vision is to drive information and technology solutions at the pace of American innovation. It would be a huge failure on my part if the attorney general could go to Best Buy and buy something better than what I'm providing. We also want to be known as wise stewards of taxpayer dollars, so being frugal and smart with our investments. We want to be bold enough to make a difference. We need to be adaptive because we're embracing and leveraging the changing world. We need to be smart risk-takers who experiment wisely with technology. We are technology leaders whom people trust because we exceed expectations.

We are in the process of revising our strategic plan, and we have four goals. The first is continuous service delivery improvement. It's ongoing and something you always want to focus on. Make sure you're trying to do everything you can to drive customer experience and provide tailorable services. At the same time, we want to provide enterprisewide services. We want to build intelligence and automation into standard processes. In so much of today's IT environment, you've got to react fast, mostly in real-time. We want to strengthen and forge strategic relationships with our business partners. They're every bit as critical to our success as our own employees. We want to design and launch autonomous services to support mission critical operations.

Secondly, we need to manage taxpayer funds wisely. I'm focusing on how we maximize the value from our budget. We want to pursue cost savings through shared services while exercising spending authorities that really pave the way for efficient modern systems. The key is strengthening cost transparency, accountability, and performance. I focus on leveraging economies of scale through strategic sourcing and partnering with other parts of the government to do that. We need to remove unnecessary layers of complexity and proprietary solutions. Open source standards-based solutions are ultimately going to be more cost effective.

The third one is protecting the mission. We want to minimize the risk through continuous monitoring. We want to enhance our enterprisewide instant response and cyber hunt capabilities. I want to provide enterprisewide identity credential access management services to ensure that the right users are accessing the right information and that we have the right credentials in place. When you talk about



“In addition to modernization, the concept of transformation speaks to adopting technologies and strategies that fundamentally shift how agencies do work. The last thing you want to do is just modernize the existing systems that you have in place with the same processes. You also need to create a dynamic IT environment that can evolve as your enterprise does.”

—Joe Klimavicz

protecting the mission you have to have plans in place for IT recovery, reconstitution, and business continuity of our key operations.

Our final goal is maximizing mission capabilities. I position my office as full service. We’re driving department-wide access and management of our smart data. It is about realizing the potential of dark or unused data. There is a lot of data that’s collected for a one-time purpose and then essentially put on a shelf. I want to make sure that we’re maximizing the use from this information. We are improving operations and stakeholder experience incrementally through micro innovations. Micro innovations, pilots, or proof of concepts are a great way to bring in new technology.

You can’t talk about data without talking about analytics and machine learning. We have tremendous amounts of information, much of it unstructured, and we’re constantly bringing in and evaluating new analytical tools.

IT modernization is a key priority for the Trump administration. I’d like to explore your efforts in modernizing the infrastructure and systems at DOJ. Would you tell us more about your migration to the cloud? What are the benefits?



The push to IT modernization coming out of the White House, with support from the Hill, is allowing CIOs the opportunity to address challenges head-on. The centerpiece of our modernization efforts has to start with what we built out as a cloud-optimized trusted Internet connection service. We essentially have a dual security stack, one going out to the regular Internet and one going to our business partners that are providing cloud services. This provides a secure direct access to our cloud service providers at very high speeds. Everything is fully redundant, very robust. If you’re going to say cloud is everything, then you have to build that network access to your cloud partners. We’ve also accelerated the adoption of cloud email. We’re very close to completing the move for all of our offices to Microsoft 365. When I came to Justice a little over four years ago, we had about 23 different email systems. We reduced that down to nine. Now we’re very close to getting that down to one. We’re saving the department tens of millions of dollars

annually. At the same time, we are facilitating cross-component collaboration because we’re essentially on one platform.

The benefits of cloud have been articulated many times. To me, it is unfettered secure access across all of your devices and locations. In the DOJ, we have about 2,400 locations around the world where we have folks stationed. You really need to provide access from all of these points. It also centralizes our infrastructure platform, so it allows easier access to user information, where it is housed, and collaboration. We can leverage the cloud infrastructure, reduce redundancy, and the automatic failover is something that’s key. Operational efficiency and enhanced security are all things that are critical to supporting our core missions.

Some of our key mission systems are also taking advantage of the cloud. I’d like to highlight a couple. Within the FBI, the National Crime Information Center modernization is delivering new search capabilities and matching algorithms to a system that was deployed nearly 20 years ago. We’ve made a lot of enhancements to the National Instant Background Check System (NICS), enabling faster and more accurate dissemination of gun purchase eligibility. We’re modernizing our next generation identification infrastructure as well to improving the response, biometrics analysis, and identity confirmation. Within the United States Marshal Service, it is modernizing its case management system, a program called CAPTURE focused on custody management, prisoner transport, and fugitive case management. It is a huge payoff in terms of enabling system-to-system interoperability and information sharing. Within our Executive Office for Immigration Review, they’re also updating and modernizing case management capabilities. This enables immigration judges to reduce the backlog of immigration review cases. So much is happening that changes how we do business.

Cloud migration presents significant challenges. Would you like to share any challenges faced in migrating to the cloud?



The move to the cloud presents several challenges. I’ll highlight a couple. Early communication with all stakeholders is vital. The stakeholders must be aware of the goals, outcomes, and major milestones that are going to

occur during the migration. I regularly meet with component CIOs to address these challenges. You have to get that messaging for the migration to be mission centric. It is not simply about IT, but it's about doing something better so that the department can operate better.

Enterprise security is another key step that has to be addressed. In the old days, organizations could pretty much count on a well-defined security boundary and build that security boundary into their network. Cloud services provide flexibility, and require a different way of looking at security. Current cloud breaches have been mostly due to poor configuration, lack of visibility, and lack of knowledge of how to properly defend cloud environments. We're actually looking at a holistic cloud security infrastructure that delivers that visibility and responsive capability. I think if you're buying software-as-a-service in a cloud environment, then the cloud provider should provide the entire security. Often we're doing infrastructure or platform-as-a-service with the industry partner in securing the infrastructure—but we still have to secure the application that's riding on the infrastructure.

Another aspect is the network. Everything is remote by definition. You need to make sure you've got sufficient bandwidth, not only for your current workload, but also for your future data growth. A robust and secure network is absolutely critical as you move to a cloud environment. The most significant and most overlooked issue is the people. The mission owners can be reluctant to physically separate from their servers. Again, it's impossible to over-communicate. You need to be sensitive to the human aspect inherent in this migration.

Some of the lessons learned involve consistent priorities, good inventory of what you have, developing a migration plan and schedule early, and prioritizing the mission first. You can have the greatest optimization plans, but those plans can't interrupt the agency's mission. The mission will always come first and it must. Some of the benefits are ubiquitous access to data and computing. We've got a chance with cloud to aggregate the information, the compute, and the analytics together in one place—and that's very powerful. Lastly, computational accelerators such as quantum and neurocomputing will be critical to fully secure and leverage capabilities. These cutting-edge computing technologies, like quantum, are only going to be available on a cloud environment.

Why is modernization not enough? What are the implications of a digital transformation?



Modernization is really important, but if you limit your efforts to only modernization, you're going to limit your gains in terms of performance and security. In addition to modernization, the concept of transformation speaks to adopting technologies and strategies that fundamentally shift how agencies do work. The last thing you want to do is just modernize the existing systems that you have in place with the same processes. You also need to create a dynamic IT environment that can evolve as your enterprise does. A key aspect of this is creating a high performing, nimble workforce that can understand the technology, understand what is possible.

To learn more about the U.S. Department of Justice's Chief Information Officer, go to justice.gov/jmd



To hear *The Business of Government Hour* interview with Joe Klimavicz, go to businessofgovernment.org.



To download the show as a podcast, go to PodcastOne, iTunes, and businessofgovernment.org.



To view excerpts of the show, go to youtube.com/businessofgovernment.



To read the full transcript of *The Business of Government Hour* interview with Joe Klimavicz, go to businessofgovernment.org.