September 20, 2017

Christopher Liddell
Director, American Technology Council
The White House
1600 Pennsylvania Avenue
Washington DC 20500

Director Liddell:

Oracle appreciates the opportunity to provide comments on the Administration's plan to modernize the Federal Government's information technology environment. Executive Order 13800 sets out a range of priorities for departments and agencies, acknowledging the essential role of IT modernization to address cyber security risk management for the government and the nation's critical infrastructure. The American Technology Council's (ATC) Report to the President on Federal IT Modernization (the Report) takes the key step of engaging the private sector to benefit from the range of expertise and perspectives available. We strongly commend the transparent and inclusive process employed by yourself, Jared Kushner, and Reed Cordish in all your work on the ATC.

Regarding the report, we applaud the general themes of 1) moving to cloud to transform the security and functionality of federal IT systems, 2) defend data, not just the network perimeter; and 3) consolidating services, where appropriate, to increase efficiency and reduce cost.

We respectfully suggest the government has not gone far enough in articulating a plan that will result in significant change and instead seems to be driving the government in the opposite direction. Many of the Report's recommendations and current modernization efforts seem out of sync with the best technology practices deployed in a Fortune 50 company today. This Report wasn't prepared in a vacuum, but rather is part of a larger attempt to transform government IT that predates the Trump Administration. It is our view that both this Report and those efforts are not only likely to fail, but also put the taxpayer at substantial security risk.

We agree entirely that the delta between the private sector's use of technology and the government's use of technology is too large. The fact is that the efficiency, security, and both user and customer experience of private sector deployed technology is at least a decade ahead of the government. The USG has an opportunity to leverage those experiences. Yet, the USG is not adopting the critical lessons learned by the private sector, instead pursuing initiatives abandoned long ago by the private sector.

In addition, the actions of the USG seem to misdiagnose the two major events driving modernization, the Healthcare.gov failure and the breach at the Office of Personnel and Management. Without question, the OPM and Equifax security breaches underscore the

USG's responsibility to protect data and secure systems given the unimaginable costs of these intrusions.

Further, the actions of the USG and much of what is contained in the Report ignore the fact that labor is the single greatest economic driver in IT. Therefore, custom code that increases labor costs to build, maintain and patch, will *not* result in substantial cost savings. The goal of modernization should be to leverage the substantial investment of the private sector to avoid development and labor costs, not to attempt to emulate the technology development of the private sector.

Last, there is very little attention paid to the basic blocking and tackling of defining, evaluating, competing, and choosing technology on its merits that has always served the government well, and is the mainstay of technology procurement in the private sector. Competition seems to be set aside entirely.

There are three false narratives that have taken the USG off course in our view:

1) False Narrative: Government should attempt to emulate the fast-paced innovation of Silicon Valley. Silicon Valley is comprised of IT *vendors* most of which fail. The USG is not a technology vendor nor is it a start-up. Under no circumstance should the USG attempt to become a technology vendor. The USG can never develop, support or secure products economically or at scale. Government developed products are not subject to the extensive testing in the commercial market. Instead, the Government should attempt to emulate the best-practices of large private-sector Fortune 50 *customers*, which have competed, evaluated, procured and secured commercial technology successfully.

2) False Narrative: In-house government IT *development* know-how is critical for IT modernization. In-house government *procurement* and *program management* expertise is central to successful modernization efforts. Significant IT development expertise is not. Substantial custom software development efforts were the norm at large commercial enterprises, until it became obvious that the cost and complexity of developing technology was prohibitive, with the end-products inherently insecure and too costly to maintain long-term. The most important skill set of CIO's today is to critically compete and evaluate commercial alternatives to capture the benefits of innovation conducted at scale, and then to manage the implementation of those technologies efficiently. Then, as evidenced by both OPM and Equifax, there needs to be a singular focus on updating, patching, and securing these systems over time.

3) False Narrative: The mandate to use open source technology is required because technology developed at taxpayer expense must be available to the taxpayer. Here there is an inexplicable conflation between "open data," which has a long legacy in the USG and stems from decades old principles that the USG should not hold copyrights, and "open source" technology preferences, which have been long debated and rejected. There is no such principle that technology developed or procured by the USG should be available free for all citizens, in fact that would present a significant dis-incentive to conducting business with the USG.

These false narratives have led to a series of actions that is unquestionably holding the USG back from modernizing its IT, some of which are contained in the Report, but all of which are being deployed across government, to the bewilderment of many in the private sector.

1) The largest contributor to cost and complexity is *customization*, yet actions of the USG and the Report seem to embrace both government developed bespoke technology *and* customization. Custom code needs to be maintained, patched, upgraded and secured over the long-term. The cost of technology comes almost entirely from labor, not from component parts, whether software, hardware, or networking. The goal should be to seek leverage and scale by engineering out labor costs, including process engineering. Government developed technology solutions must be maintained by the government. Every line of code written by 18F, USDS or another government agency creates a support tail that results in long term unbudgeted costs.

2) Very little in the Report focusses on *process* modernization and reform. Before a single line of custom code is developed, the USG must modernize process to adapt the commercial best practices that are embodied in commercial off the shelf software. This is particularly true in the context of shared services and cloud Software as a Service (SaaS), which first require a baseline of shared processes across agencies. Unique, government-specific processes are one of the main culprits for IT cost overruns.

3) Technology preferences and mandates seem to have replaced *competition*. Even though technology preferences have long been rejected by USG policymakers, it appears that technology preferences are experiencing a resurgence in the USG. Technology preferences rob the USG of the benefits of competition for features, functions, price, security and integration just at the time that technical and business model innovations are occurring rapidly. Declaring *de facto* technology standards without robust competition not only skirts government competition mandates but places the government at substantial risk of failing to acquire the best, most secure and cost effective technology, even if those *de facto* standards are proposed by well-meaning government employees who “came from the private sector.”

4) Many of the technology *preferences or mandates* include open source software. Open source software has many appropriate uses and should be competed against proprietary software for the best fit and functionality for any given workload, but the fact is that the use of open source software has been declining rapidly in the private sector. There is no math that can justify open source from a cost perspective as the cost of support *plus* the opportunity cost of forgoing features, functions, automation and security overwhelm any presumed cost savings. The actions of 18F and USDS plainly promote open source solutions and then propagate those mandates across government with the implicit endorsement of the White House. The USG’s enthusiasm for open source software is wholly inconsistent with the use of OSS in the private sector.

5) The focus in the Report on *security* seems *out of sync* with the threat USG systems face and the very substantial cost of data breach. Data security frameworks have moved far beyond multi-factor authentication, to leverage control of data on a granular level, to protect against the insider threat and to utilize artificial intelligence to identify intruders and automate defenses. Moreover, the initial development and adoption of login.gov is an example of misdirected security resources leaving taxpayers without state of the art single-sign-on best practices and technology.

6) Developing custom software and then releasing that code under an open source license puts the government at unnecessary security risk as that code is not "maintained by a community," but is rather assessed and exploited by adversaries. Further, this practice puts the government – most likely in violation of the law – in direct competition with U.S. technology companies, who are now forced to compete against the unlimited resources of the U.S. taxpayer. The Equifax breach stemmed from an exploit in the open source Apache Struts framework.

7) The Report's and the USG's focus on setting guidelines for how to *build custom applications* – "agile" development on open source following the "playbook" -- is fundamentally at odds with the approach of private sector enterprises. It creates a development and procurement bias that promotes results-oriented outcomes, regardless of whether those outcomes are in the best interest of the taxpayer.

8) The USG's initiatives to recruit engineers from private vendors has resulted in the predictable outcome of creating favoritism for those vendors' solutions, and seems to replace presumed technical expertise with the more complex task of procuring, implementing, maintaining, and securing systems over the long term.

9) The Report does not address the true *acquisition problems*, and even risks adding new layers of valueless bureaucracy. Aggregating buying power through a dashboard on a per-unit basis to achieve volume discounts does not model the private sector's approach to acquisition. Per-unit discounts do not account for a buying position that is capable of demanding holistic solutions by realizing discounts across units and functions. The dashboard approach also does not capture the cost to migrate an existing system to a new system, and per-unit discounts cannot capture the pros and cons of highly-differentiated IT products, because the dashboard does not consider the technical, architectural and security capabilities of products. The fact is that there is no analog to a dashboard or a "marketplace" in the private sector for differentiated IT products because those products are best procured through vigorous evaluation and competition.

Even though the Report repeatedly cites its' preference for private sector solutions, this really only comes through in the Report's focus on cloud. Here, again, we cannot stress enough the importance of rigorous competition. The fact is cloud technology models, licensing models, pricing models, and delivery models are changing and innovating rapidly, particularly in Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). But at the same time the Report embraces competitive cloud solutions, it endorses a *de facto* government PaaS standard in its implementation of Cloud.gov and

then further puts the cloud.gov solution in direct competition with private sector PaaS solutions.

Additionally, it seems clear that public cloud is not the correct course for most USG solutions, and the best answer is some combination of hybrid and private cloud, which may also take on characteristics of managed services. It should be the government's policy to maintain ongoing competition between and among each of the different vendor's approaches to technology, licensing, and pricing.

If the Administration is serious about closing the digital delta between government and the private sector, it must do the hard work of process and procurement reform; it must abandon the idea of "government as a vendor," in favor of "government as a customer;" it should recognize that projects like marketplaces with no commercial analog, development projects like logon.gov which already exist in the commercial sector, and technology preferences (in many case mandates) like cloud.gov and open source really need to be rethought immediately.

We have attached a response to each of the questions asked and the RFI below. We are happy to discuss our response at any time, or to provide the government with additional information.

Sincerely,

Kenneth Glueck
Senior Vice President
Office of the CEO
Oracle

ORACLE

Oracle Response to Posed Questions

1. **What are major attributes that are missing from the targeted vision?** (Appendix A, Appendix B);

With respect to Appendix A: Data-Level Protections and Modernization of Federal IT, we believe the notion that a small set of security controls should be prioritized is misplaced. The Federal government has information that no other entity in the world possesses. As such, it will be targeted by the most sophisticated adversaries. Thwarting these adversaries requires sophisticated capabilities, with security built-in from the code base on up, really from the silicon up. We therefore make two recommendations with respect to Appendix A:

- *Adopt the Entire NIST Cyber Security Framework*. The capabilities described in Appendix A are a good collection of best practices; however, as presented, they do not represent a Data-Level security model. Both the Foundational Capabilities and the Risk-Based Capabilities are generally considered to be basic security hygiene and represent only a subset of the requirements contained within the NIST Cybersecurity Framework, which the Administration has highlighted as the basis for cybersecurity risk management in EO 13800. Oracle believes the NIST Cybersecurity Framework is a valuable tool and recommends that it serve as the basis for the important security capabilities implemented as part of IT Modernization. Implementing the NIST Cybersecurity Framework is made easier in cooperation with Cloud Service Providers who not only have met its requirements for their products but can demonstrate it with data.
- *Leverage Data Control Functions.* Legacy systems protect data by setting up a security perimeter around it and trying to control access to the database through a firewall. In even a medium-sized government organization, that can mean thousands of servers and thousands of firewalls protecting them. As projects end and staff rotate, updates and administration becomes nearly impossible. To secure data, Federal agencies need to be able to control access to it on a granular level. They must be able to do so in a way that is seamless for those that are authorized to access it and impossible for those who lack authorization. With today's modern database architectures, independent databases can be hosted within a single, secure data base container with identity and access controls integrated. One system to update; one system to maintain with custom security controls for each database instance. Access controls can be pushed down to very granular levels and, administrative rights can be controlled in ways that allow administrators to do their jobs without granting them access to the data managed on the system, therefore protecting against the inside threat. Data can be encrypted at rest, in transit and while being accessed. Immutable audit logs – logs that can't be changed by malicious insiders or external adversaries trying to

cover their tracks – are designed into these systems, allowing for strengthened compliance, alerting on anomalous activity, and, on a bad day, faster forensics.

With respect to Appendix B: Principles of Cloud-Oriented Security, Oracle applauds the focus on Cloud-Oriented security; however, Oracle believes that the proposed model is simply re-creating the perimeter-based approach at the data center instead of taking a truly "data-centric" approach. While the Appendix notes that this proposal is for agencies building applications on top of cloud infrastructure and does not apply to Software as a Service (SaaS), a better approach than replicating network-layer security in the cloud would be to build in the security functionality provided by commercial SaaS applications (or to simply acquire commercial SaaS applications).

A truly data centric approach limits access down to the data to the cellular level. It then uses continuous monitoring to automatically detect and block access when accounts are compromised and uses machine learning to further detect potentially malicious behavior. By utilizing modern SaaS applications, Federal agencies can simply turn on multi-factor authentication, and be assured that basic hygiene like secure configurations and vulnerability management are occurring automatically by the cloud provider. To verify that these actions are taking place, Federal agencies can receive and monitor data on the status of these actions. Oracle highly recommends that DHS and the Office of Management and Budget develop guidelines for custom-built Cloud applications that ensure they are built with the same security functionality and to the same high standards as competing commercial applications.

2. **What are major attributes that should not be included in the targeted vision?** (Appendix A, Appendix B)

As noted above, Oracle does not believe that a small subset of controls can provide the Federal government the necessary level of security; nor do we believe that "the Principles of Cloud-Oriented Security" are in fact principles for the cloud but simply the porting over of a network-based security model appropriate for legacy systems. The target vision should not focus on how to secure custom-built applications on cloud platforms but on the adoption of secure, commercial cloud applications.

3. **Are there any missing or extraneous tasks in the plan for implementing network modernization & consolidation?**

A. Modernizing FedRAMP

Rapid modernization of Federal IT systems will not be possible without a rapid move to secure cloud-based applications. Beyond determining technical controls, the final report to the President needs to address process problems that make it difficult for Federal agencies to move to the cloud. Chief among these problems is the Federal Risk and Authorization Management Program ("FedRAMP"). The missing task for this report is a plan to streamline FedRAMP and move to a continuous monitoring approach for verifying security requirements in the cloud.

FedRAMP was meant to simplify the procurement of cloud services by providing "a government-wide program that provides a standardized approach to security

assessment, authorization, and continuous monitoring for cloud products and services." Utilizing a "do once, use many times" framework, FedRAMP is supposed to save the government money. While the approach is fundamentally sound, execution has been poor and the results less than stellar. The existing FedRAMP program has a paltry 80 offerings, a small fraction of the offerings available in commercial cloud markets or directly from cloud providers, replacing only a small number of the 200,000+ software products Federal agencies procure. Seven years after the Obama Administration announced a Cloud First policy that would move $20 billion of Federal IT spending to the cloud, the latest estimates put Federal spending on cloud services well short of that goal.

The onerous accreditation process is both costly and unnecessary. In 2014, FedRAMP accreditation took an average of nine months and cost providers $250,000; in 2015, the process was taking an average of two years and as much as $5 million. The process is also opaque to vendors, who do not receive timely updates on where they are in the approval chain and are unable to solicit information from Federal officials.

The security assessment process uses a standardized set of FedRAMP requirements in accordance with the Federal Information Security Management Act ("FISMA"), 44 U.S.C. § 3541 et seq., and National Institute of Standards and Technology ("NIST") Special Publication ("SP") 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, to grant security authorizations. These standards are widely regarded as best practices within the cybersecurity industry; however, the assessment of implementation of these standards is onerous and ineffective.

The process begins with vendors completing a System Security Plan (SSP). FedRAMP provides a word document template for each of the accreditation levels (low, medium, high). The Low Baseline template alone is 175 pages and 36,000 words. The High Baseline template is 350 pages and 80,000 words. The Veris Group, a third party accreditation organization, warns potential clients that a completed SSP is likely to be over 750 pages.

This kind of paper-based, static security review is outdated and unnecessary. Compliance documented on paper does not equal security in the real world. Recognizing this reality, the FedRAMP program office (along with other Federal agencies) have established a Continuous Monitoring program that monitors over 50 controls following accreditation. Most of these however, do not provide a continuous flow of data but are simply monthly or annual requirements.

The initial accreditation process should move from word document templates to real-time monitoring of vendor implementation of controls. Responsibility for monitoring the security of vendors should be moved from the FedRAMP program office to the Department of Homeland Security (DHS). DHS is vested under Federal law with responsibility for protecting civilian Federal agencies. Continuous monitoring of FedRAMP vendors should be part of US-CERT's mission to protect Federal agencies.

Under this model, DHS should standup a dashboard for monitoring the security of FedRAMP vendors. Access to the dashboard for a FedRAMP service should be available to both the vendor and Federal agency users. The accreditation process should begin with the vendor completing initial data submission on the dashboard

website, eliminating word documents. As the vendor connects data feeds to the dashboard, compliance with the monitored controls can be reported in real time using a stop light protocol (red for no data, yellow for data that shows non-compliance, green for compliance).

DHS should work with vendors to develop new controls to expand the number of requirements that can be monitored in real time.

B. Using the Cloud to Realize the Vision for Security

As a Cloud Service Provider and data storage, processing and security company, Oracle is not best positioned provide advice on improving Perimeter-Based security approaches. Our comments are therefore directed at addressing how many of the goals of Perimeter-Based security can better be met through partnership with Cloud Service Providers.

a. Cloud Security and Situational Awareness

Use of Cloud infrastructure and applications can provide the Department of Homeland Security far better situational awareness than can be gained through a perimeter-only based approach. Beyond replicating this level of visibility, Oracle can, as a technical matter, provide DHS and Federal agency clients, additional data at the infrastructure, platform, and application layer to create a clear view of not only threats but the state of security tools and configurations.

b. Encrypted Network Traffic

Solutions to addressing encrypted network traffic either rely solely on using meta data to identify potential malicious activity or must decrypt the traffic to inspect it. Both approaches are problematic. Use of meta data leads to high false positives and so, in most organizations, is only used to "detect" potential malicious activity, not to stop it. In contrast, decrypting the traffic can provide higher fidelity security but introduces a multitude of problems including high latency and exposure of data to unauthorized parties. A better approach is to move the security activities to the point at which the data is decrypted for its intended use. By moving these security functions to the application layer, data is not decrypted in transit. In addition, the context is available to make informed security decisions through automated processes as described below.

c. Overreliance on Static Signatures

For Oracle's enterprise security, we have moved away from systems that can only stop known threats and built or implemented systems that can identify patterns of anomalous activity that may indicate malicious intent. This approach requires the gathering and analysis of large volumes of data and is most effectively done not at the network layer but at the application layer. Oracle would be happy to provide the Office of Management and Budget a briefing on this approach.

d. Use and Value of Classified Indicators

Oracle recognizes the use and value of classified indicators. Oracle does not see any barriers to instrumenting its Federal offerings to use these indicators. There is no reason that a Cloud provider offering email-as-a-service could not direct mail to be

filtered through an Einstein 3A sensor. While Oracle does not offer email-as-a-service, it's applications that rely on DNS could be filtered through Einstein 3A either on premise or at a third party location. Additional countermeasures could likely be implemented as well.

e. Continuous Diagnostics and Monitoring

As discussed in our comments on FedRAMP, the goals of the Continuous Diagnostics and Monitoring (CDM) program that have been difficult to realize on legacy architectures can be readily achieved in cooperation with Cloud Service Providers. Enterprise cloud platforms can provide the data necessary for CDM in real-time. While CDM has been focused on a limited number of controls (four to five), many more can be monitored using data feeds from Cloud. Oracle has mapped out the data feeds that can be used for continuous monitoring, and concluded that 37 of the 98 categories of the NIST Cybersecurity Framework could be monitored continuously. Aspects of an additional 50 control groups can be monitored with such an approach.

4. Are there any missing or extraneous tasks in the plan for implementing shared services to enable future network architectures?

Oracle applauds the approach outlined on shared services, in particular the sound endorsement of cloud services. As the report notes, "Agencies must leverage shared services and embrace commercial technologies where possible, building new capabilities only when shared services and commercial technologies cannot meet mission need." In our experience working with the Federal government, there are few circumstances in which it will be more efficient or cost effective to use a "shared service" model (where a Federal agency performs services for other Federal agencies) over adoption of enterprise-grade cloud services that can meet both the business and security needs of Federal agencies.

5. What is the feasibility of the proposed acquisition pilot? (Appendix D)

The pilot program described in Appendix D proposes to aggregate the pricing of government-wide email by enabling agencies to buy email licenses from a price point submitted by each vendor to a government-wide dashboard. The agency and contractor would not negotiate. As we understand it, the Report speculates that the government will achieve greater discounts by placing email providers in direct, live competition and by pricing discounts based on government-wide volume, rather than relying on individual agency negotiation. The Report is particularly concerned with increasing the negotiation power of small agencies.

The Report is correct that acquisition reform is needed. Government needs more agile buying power and contractors need the ability to sell quality products and services at a competitive price. The complex web of acquisition laws and regulations that currently establish the relationship between the government and its vendors undermines these goals, making even simple acquisitions of commercial items an expensive chore. In many instances, the acquisition process prohibits government from procuring the most innovative products available in the market place (a fact especially true of information technology systems that change continually). However, the Report's solution to aggregate government-wide buying power into a marketplace dashboard does not significantly improve the procurement process or results. It does not move government toward commercial-market buying. Specifically, the Report fails to meaningfully address:

- The cost and technical capabilities for migrating existing IT structures;
- The highly differentiated technical capabilities of complex IT products and the packages designed for a given function;
- In general, factors other than cost broken out by unit; and
- Competition laws that still require the full procurement process and already provide for government-wide volume discounts (even by small agencies!).

Rather than focus on adding yet another technology layer, IT modernization should focus on tackling the difficult issues in the procurement process that truly impede government from adopting commercial market buying methods. Two reforms are needed to achieve more agile, impactful buying power for the government:

1) government must eliminate regulations and contract terms and conditions that increase the cost of compliance (on both the Government and the private sector) and limit the number of vendors willing to directly contract with the government; and

2) government must organize its agency purchasing pools by function, giving consideration first to what functions each agency needs and which agencies share those functional needs.

Thus, the first step in IT Modernization is for agencies to consider what IT functions they need to procure and whether those functions should move to the cloud. Agencies should then issue joint competitions among all similarly positioned government stake-holders for those functions, and award task orders to vendors that comprehensively offer the best value to the government in both technical capabilities and cost for the specific functions needed by an agency. In this way, government is eliminating duplication, and getting the most for its money by truly leveraging buying power a macro level, rather than merely looking for volume discounts on per-unit basis (as is already done at GSA).

A. <u>What is Missing in the Report</u>

a. Transparent, Accurate Cost Assessments

First, the pilot program in Appendix D suggests that agencies will be able to order email licenses from a dashboard and start using a certain email technology instantly at the total price per unit listed. This instantaneous acquisition method cannot possibly take into account migration and integration costs that cannot be assessed without additional information regarding legacy systems. The cost to migrate will depend on the infrastructure of the product purchased from the dashboard, so agencies cannot effectively scope the cost of migration prior to ordering from the dashboard.

b. The Technical Differences in Products

Second, as the Report points out, cloud is not a commodity. The pilot program described in Appendix D does not account for technically complex, highly-differentiated products. Complex IT products cannot be sold off a dashboard. The commercial sector leverages holistic packages of software-as-a-service offerings for various products that knit together the functions that are able to provide synergy. In fact, there is no

articulation—let alone comparison of—technical strengths and weaknesses on the proposed dashboard. It is unclear to us how the Acquisition Tiger Team described in the report would be able to conduct meaningful analysis for complex IT cloud products if the team's analysis is based on base-line, single-unit products. As has always been done in the past, contractors must provide information on what the contractor is technically capable of providing. The government should focus its technical expertise in helping agencies understand the technical proposals that are submitted by contractors through the traditional procurement process.

c. Longstanding Competition Requirements

Third, the Report does not address how Appendix D's pilot program will streamline competition requirements. Under Competition in Contracting Act ("CICA") of 1984, 10 U.S.C. § 2304(a)(1)(A) & 41 U.S.C. § 3301(a)(1), the Clinger-Cohen Act ("CCA"), 40 U.S.C. § 11101 *et seq*, and Federal Acquisition Regulation ("FAR"), 48 C.F.R. Part 6, agencies are required to engage in "full and open competition" for acquisitions above the simplified acquisition threshold (currently $150,000). "Full and open competition" requires the government to allow all responsible offerors the opportunity to compete for the work. FAR 2.101. The requirement that government engage in competition extends to pre-negotiated multiple-award, indefinitely-delivery, indefinite-quantity ("IDIQ") contracts, 41 U.S.C. § 3302, under which the government is required to provide "fair notice" and "fair opportunity" to all qualified contract-holders to compete to fulfill a particular task order.

Because of these competition requirements, Congress has specifically empowered GSA—by statute—to be a government-wide purchaser, using a streamlined procurement approach. *See* 40 U.S.C. § 501 (authorizing GSA to "procure and supply personal property and non-personal services for executive agencies to use in the proper discharge of their responsibilities, and perform functions related to procurement and supply[.]"). GSA interprets this statute to require agencies to issue a Request for Information ("RFI") for purchases above $150,000 (the simplified acquisition threshold). Under this process, vendors submit commercial pricing for commercial items to GSA. GSA negotiates government-wide price lists of commercial items (called "Schedule Contracts"), and these prices are then determined "fair and reasonable" under law. Any agency can purchase from a negotiated schedule at any time – including small agencies.

i. Aggregate Buying Power by Unit is a Historically Failed Solution

Therefore, the Report fails to acknowledge that this "aggregate buying" approach exists today at GSA. GSA negotiates set pricelists that require sellers to provide not just the best price for a government user, but to make the government the most favored customer even against commercial customers. The government usually receives a set percentage discount below what has been determined to be the analogous vendors, a requirement called the "price reduction clause." Thus, the Report seems to adopt the exact same approach to "curing" procurement ails as the government has tried in the past – leverage government-wide buying with standard terms and conditions. This approach has been done before.

What the Report is silent on, that may have significant impact on the market, are removing restrictive, onerous legal terms and conditions contractors are currently subject to that serve as a barrier for many contractors to enter market, such as the price reduction clause. Importantly, it is the elimination of these onerous requirements that would cause a change to the market – not the mere leveraging of governmentwide purchasing on a product-by-product basis, which is already done. Oracle strongly recommends that government negotiate commercial terms and conditions with industry in advance of adopting this pilot program so that it can be determined whether significant market impact through true procurement reform can be realized.

ii. The Proposed Dashboards Do Not Streamline General Competition Standards

Putting aside GSA, the government-wide dashboard concept included in Appendix D either does not meet basic competition standards, or still requires agencies to undergo a full competition (it was not clear to us which outcome would be the case). The dashboard itself enables agencies to look at only one metric – unit price based on a certain volume. This metric says nothing about technical, past performance or security metrics. The government must give significant consideration to how contractors would be given "fair notice" of how they would be evaluated under some sort of shortened procurement process, and then how agencies would cull the necessary technical and security information for each offering such that all vendors are given "fair opportunity" to participate. It is not clear to Oracle how the dashboard changes the traditional procurement process beyond mere price-setting.

B. The Revolutionizing Solution: Adopt Commercial Practices of Leveraging Buying Power to Demand the Best Full Solution Commercial Contracts

The federal government does need to streamline procurement, but not by creating one more technological layer. Rather, the federal government needs to return to acquisition basics, focusing first on the government's internal process of deciding that functions it needs to purchase. Each agency should inventory the functions that it needs. The government can then examine which functions and which agencies are similarly situated, and then appropriately pool user bases (*i.e.,* specific federal agencies) through inter-agency agreements under the Economy Act, 31 U.S.C. § 1535 and FAR 17.501, and standing up multiple-award IDIQ contracts that cater to those groups' cloud requirements. One pool of federal agencies (e.g., DoJ, DHS, FBI) could conduct a joint competition for one type of cloud that is best suited to their tasks; simultaneously, some of those same agencies (DoJ, FBI) could work with other agencies (CIA, NSA) to focus on a separate competition to obtain a cloud that is suited to a different task. Small agencies would be given the procurement expertise and leverage of the larger agencies that they functionally align with. In this way, just like the commercial sector, the government would negotiate for discounts not based on an individual unit, but with the leverage of an entire package of products that will reap both maximum discounts and technical optimization by removing integration costs and security challenges. Thus, it is the mere categorization of critical functions and pooling of agency resources that is transformative. Government contracts should be used to support the negotiated deals, not as an arbitrary filter and driver.