WHITE PAPER

Strategic Options for **Federal Data Center Hardware Maintenance.**

PARK PLACE TECHNOLOGIES

ParkPlaceTechnologies.com

Executive Summary

COVID-19 has impacted the federal government and its approach to technology for years to come. Infrastructure managers face significant budget pressures, have stretched thin teams, work remotely and deal with travel restrictions. With a new President and agenda, priorities will change even further to bring to life campaign promises. At the same time, infrastructure teams ensure they are keeping the lights on with existing equipment.

Federal government infrastructure managers need to find ongoing cost savings and free up time to work on high priority initiatives. Now is a great time to consider utilizing a third-party maintenance (TPM) provider. TPMs provide support programs for top tier OEMs and are vendor agnostic. Infrastructure managers can take advantage of cost savings of up to 30-40% while working with only one partner focused on keeping your data centers up and running. TPMs provide hardware monitoring across the federal department's infrastructure with automated issue detection combined with actionable insights so appropriate action can be taken.

TPMs already provide services to many federal government agencies and departments. Federal infrastructure managers should look for TPMs with significant experience across departments and operations wherever you need them in the U.S. or globally. Locate a TPM with an existing GSA contract in place for required MSA schedules to ensure excellent communication and pricing right away. They should also be FAR compliant and have necessary security clearances in place.

Infrastructure managers can take advantage of cost savings

of up to 30-40%

PARK PLACE TECHNOLOGIES

Budget Pressures

The impact of COVID-19 had far-reaching implications across the entire I.T. industry, with budgets dropping in 2020. It was no different for the federal government. The federal government shifted priorities to respond to the global pandemic creating massive stimulus efforts to keep the economy from collapsing. This stimulus spending will create budget constraints for many years. Further, federal infrastructure teams had to ensure government services could be provided in new ways while keeping its workforce safe during and after mandatory shutdowns.

2021 will continue with similar budget pressures. According to ITDashboard.gov[1], spending on I.T. across government agencies in fiscal 2021 will be $90.9B - only 1.79% higher than 2020. Significant spending on cybersecurity initiatives[2] continues to be the federal government priority. I.T. Modernization was a loser in the 2021 omnibus spending bill[3] receiving only $25 million. Lawmakers made requests of up to $1 billion.

Achieving cost savings in data centers has been a critical strategic pillar across all federal government branches for several years. Closing redundant data centers, and optimizing need ones, continues to be necessary. Cost-saving achievements on data centers are made publicly available, so the pressure to lower costs continues. These are adding to budget pressures as the government looks to expand investment in security-related projects.

Stretched Thin Staff

Covid-19 caused hundreds of thousands of job losses across federal, state, and local governments. According to Fortune[4], in the summer of 2020, the number of government employees was the lowest since 2001. While job losses across the United States grew, families needing assistance from various government forms increased, causing more demand for existing federal services. Employees providing services or supporting those efforts in technology were stretched thin. Federal employees working in I.T. experienced enormous stress as they found themselves with less budget and co-workers.

Travel Restrictions & Remote Work Mandates

The COVID-19 pandemic impacted federal infrastructure employees in how they could work and provide services. Travel for federal employees came to a halt at the beginning of the pandemic. It was only partially reinstated by the first half of 2021. Updates on restrictions easement and mandate relief defer to local conditions. The federal government implemented remote work mandates in federal departments and agencies to reduce virus exposure to the federal workforce. When the United States gradually started opening up after initial stay-in-place orders, safeguards were put in place when federal workers had to work with constituents to provide services. These mandates included steps such as restricting the number of people allowed in federal buildings, requiring masks and social distancing, and requiring assistance to be scheduled in advance online. Infrastructure staff quickly reacted to the need for remote working though not set up to handle. The added pressures of these travel restrictions and remote work mandates highlight the need for even more thoughtfulness in prioritizing federal employees' activities.

How TPMs Can Help Federal Agencies and Departments in the Data Center

A Single Trusted Maintenance Vendor Partner

Most federal agencies and departments' I.T. data center infrastructures consist of hardware from many different original equipment manufacturers (OEMs). Each OEM has its maintenance service programs and warranties. Infrastructure leaders in federal departments must manage all these OEM service programs; thus consuming unnecessary resources. With TPMs, Federal agencies have one partner to call for maintenance services that cover many OEMs.

Better Service and Experience

When working with OEMs, getting the support needed is often a challenge. OEMs have long triage calls designed to eliminate their product as a root cause versus actually helping the federal agency solve their pressing need. When working with a TPM, their goal aligns with the federal governments - uptime. A TPM tries to get to a root cause as soon as possible to get the support issue resolved to get you back up and running. Fingerpointing between OEMs comes to an end.

Service level agreements with OEMs are not very flexible as you must select one SLA across your products. A TPM gives federal government agencies and departments flexibility when it comes to service. Having different levels of SLAs across various locations is encouraged based on your needs.

End Pressure to Buy the Latest Equipment.

OEMs engineer hardware to last a very long time. To create obsolescence, they make end-of-service schedules to sell their latest equipment to federal service agencies. OEMs continuously try to sell the newest hardware by telling customers their hardware will no longer support the OEM. A TPM can help you with immediate support when warranties expire and provide ongoing support long after equipment goes end-of-life. Extend the life cycle of your data center hardware with a third-party maintenance provider.

Hardware Monitoring That's Action-Oriented.

Federal agencies and departments depend on its infrastructure to carry out many services to their constituents. This infrastructure is complex ranging from devices in the data center to the edge. Some TPMs provide best-in-class hardware monitoring tools that work across your infrastructure and even remotely for those that can use them. Automated hardware monitoring allows for issue detection coupled with actionable insights allowing appropriate action. Look for a TPM utilizing automation to correct issues or can automatically prepare to send an informed field engineer to fix the problem.

Significant Savings Compared to the OEM Support Plans.

Federal agencies and departments can expect to save 30-40% versus OEM support maintenance plans. Many infrastructure managers believe they need to wait for end-of-service life (EOSL) before a TPM becomes an option for savings. However, you can take advantage of these cost-savings at any time.

PARK PLACE TECHNOLOGIES

Considerations When Selecting a Third-party Maintenance Provider for Federal Services.

Experience in the Federal Space

Look for a TPM with experience in federal services. A TPM should provide the number of years that they have supported federal agencies and departments. You want a partner who understands and adheres to the federal compliance standards. Ask for a list of current federal customers. Do they have a handful, or do they work with a significant number of agencies or departments? Do they have existing relationships with the systems integrators working with your federal agency or department? These are significant indicators of the service experience your agency will receive.

General Services Administration (GSA) Schedule

Federal government agencies and departments should find third-party maintenance providers with GSA contracts, referred to as Multiple Award Schedules (MAS) categories. GSA contracted providers are legitimate federal contractors and will provide streamlined communications and optimized budget spending.

Federal Acquisition Regulation (FAR) Compliance

It is imperative to ensure your TPM provider adheres to Federal Acquisition Regulations (FAR) compliances as it relates to trade agreements and parts, including compliance with the Trade Agreements Act, Parts Origin, and Refurbished Parts. The U.S. Government mandates all providers, to federally funded contracts, are FAR compliant. These procurement regulations outline how companies conduct business with the Federal Government.

Appropriate Security Clearances

Working within federal government data centers requires service providers with appropriate security clearances. Third-party maintenance providers and their employees should have proper security clearances issued by the federal government.

Significant Savings Compared to the OEM Support Plans.

Federal agencies and departments can expect to save 30-40% versus OEM support maintenance plans. Many infrastructure managers believe they need to wait for end-of-service life (EOSL) before a TPM becomes an option for savings. However, you can take advantage of these cost-savings at any time.

Introducing Park Place Technologies

Park Place Technologies is the leading provider of post-warranty data center hardware maintenance to the Federal Government and system integrators. Park Place currently supports 21,500+ customers covering 1,092,000 assets in 110,000+ unique data centers. The company started in 1991 and is based in Cleveland, Ohio.

Park Place Technologies provides critical data center support for over 24 federal agencies and departments, including the Department of Homeland Security, Internal Revenue Service, National Aeronautics and Space Administration (NASA), Coast Guard, and Federal Communications Commission. Also, Park Place works with major systems integrators such as Leidos, Raytheon, and Lockheed Martin. Park Place has supported the federal government since 1998.

Park Place understands and adheres to the strict compliance standards associated with Federal Requirements. Park Place Technologies holds a current GSA contract through its wholly-owned subsidiary, Custom Hardware Engineering & Consulting, LLC. Additionally, they have held compliance with other third-party GSA contract holders that Park Place Technologies supports and services.

Park Place Technologies' maintenance services follow the requirements of the Trade Agreements Act (TAA). First, under FAR 52.225, our parts are ancillary to our maintenance services, which are "commercial services". The parts are not manufactured by Park Place, but rather are OEM refurbished parts sourced from US vendors by Park Place, a US company. Additionally, under the TAA, if a product undergoes "substantial transformation" in the US, then it falls outside the TAA requirements. In the case of Park Place Technologies' maintenance services, hard drives and other parts that may be necessary to complete the break-fix services do not function on a standalone basis and only work when integrated with the substantially "larger" data center equipment.

Park Place Technologies follows the below guidelines for procurement of parts:

- Park Place maintains records of the source of parts used directly or indirectly under GSA schedule contracts
- Park Place uses exclusively OEM parts purchased from pre-qualified US vendors
- All parts are OEM original and go through a rigorous inspection and testing program

Global Capabilities Including CONUS and OCONUS

Federal agencies must have coverage across the 48 contiguous states and the District of Columbia (CONUS) and often outside the continental United States (OCONUS) in Alaska, Hawaii, and the U.S. territories. Many departments must also support operations overseas. Park Place Technologies is a U.S.-based company with global capabilities across 154+ countries. Our worldwide network of 1,158,000+ parts stored in 2,400+ locations regionally, locally and on-site, allows for fast parts distribution and service. Wherever you are, and whenever the need arises, Park Place is there with our multi-lingual "follow the sun" Global Customer Support Centers, 24/7 Level 3/4 Technical Support and Client Services.

Vendor Agnostic Support

Park Place Technologies supports all Tier 1 major OEM brands in storage, servers, and networking in one consolidated maintenance contract, including brands like: Oracle (SUN), EMC, IBM, Dell, HPE, NETAPP, CISCO, Brocade/McData, LENOVO, and HITACHI.

Introducing Park Place Technologies (Cont.)

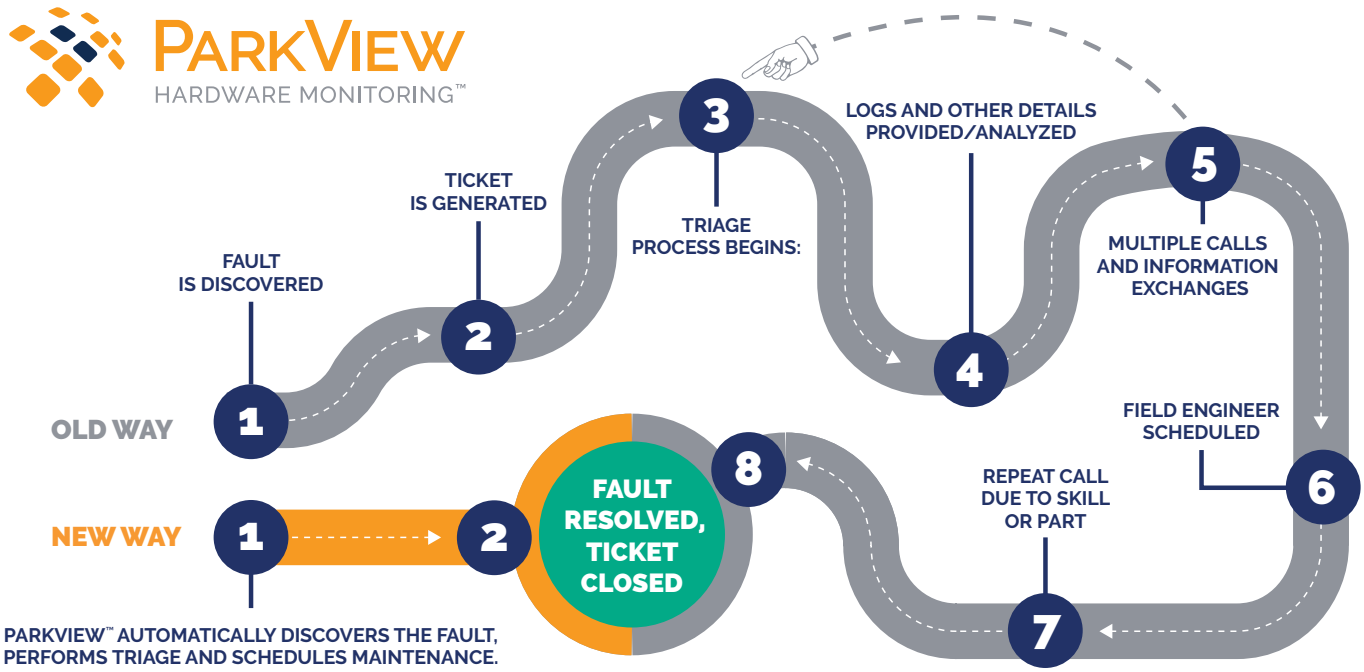
ParkView Hardware Monitoring™

Remote hardware monitoring is critical in supporting data centers in a post-COVID 19 world. ParkView Hardware Monitoring™ supports a wide range of OEMs, platforms, operating systems, and generations. Our CentralPark customer portal is an easy-to-use interface that shows real-time visibility to all events.

ParkView™ establishes a baseline standard for what each federal data center operations look like at the hardware level. ParkView™ then integrates predictive analytics to alert infrastructure teams when changes indicate potential failure. ParkView™ detects the faults for you. There is no need to contact Park Place to initiate support, run diagnostics or provide log files. This results in an incident resolution that is 31% faster than without ParkView™ and a first-time fix rate of 97%.

ParkView Hardware Monitoring™ is extremely secure and based on federal government requirements and ensure non-public data is never accessed or transmitted. Machine data is transmitted outbound to the ParkView™ monitoring infrastructure is SSL encrypted.

Simply put, ParkView Hardware Monitoring™ automates the maintenance process, resulting in faster fixes and less unscheduled downtime. Federal infrastructure teams now have more time to devote to other important initiatives.



PARK PLACE TECHNOLOGIES

Conclusion

Federal government agencies and departments have so many new I.T. priorities due to the impacts of the COVID-19 pandemic on priorities, staff, and the way work is accomplished now. With funding moving more towards cybersecurity yet pressure to achieve cost savings in the data centers increasing with modernization budgets disappearing, now is the time to consider a third-party maintenance provider to help extend data center hardware lifecycles and reduce maintenance costs from OEMs. Capable TPMs, like Park Place Technologies, have significant experience working with many government agencies and integrators and are well-versed in compliance standards. TPMs can bring capabilities that can dramatically improve the service experience while aligning to shared goals of uptime - all while reducing significant maintenance costs to keep the lights on in the data center.

Now is the time to consider a third party maintenance provider to help extend data center hardware lifecycles and reduce maintenance costs from OEMs.

[1] https://myit-2021.itdashboard.gov
[2] https://www.hstoday.us/subject-matter-areas/cybersecurity/u-s-government-to-spend-over-18-billion-on-cybersecurity
[3] https://federalnewsnetwork.com/budget/2020/12/2021-spending-bill-cyber-federal-buildings-are-winners-it-modernization-is-a-loser
[4] https://fortune.com/2020/06/06/government-job-loss-public-workers-unemployment

PARK PLACE TECHNOLOGIES