Letter of Attestation – NVIDIA Government Ready Software Program

Date: October 23, 2026

First Information Technology Services (FITS), a leading 3rd party auditing organization (3PAO), has assessed NVIDIA's Government Ready program to confirm the selection and implementation of relevant FedRAMP Class C/D/High (noted as FedRAMP High hereafter) Independent Software Vendor (ISV) controls. The primary objective of the NVIDIA Government Ready program is to provide software which meets the applicable ISV controls for use in global federal, state, local, education, and other equivalent use cases. Following its assessment, FITS attests that NVIDIA Government Ready software[1] meets the applicable requirements for FedRAMP High, FISMA High, GovRAMP High, NIST 800-53 High, and other equivalent sovereign frameworks.

Government and regulated customers have stringent software adoption criteria and limited if any ability to adopt software which is not compliant with associated environment (cloud, on-premises) level standards. However, unlike requirements for cloud and on-premises systems, there is not a recognized industry wide baseline for applicable ISV controls drawn from frameworks like FedRAMP, DoD SRG etc. Furthermore, the governmental review bodies (i.e. FedRAMP PMO or DISA etc.) do not publish applicable ISV controls for software providers to follow, nor have they coined an industry standard term for the applicable ISV controls. Therefore, customers who have FedRAMP or equivalent requirement needs don't have a standard term to refer to said controls and often do not have assurances that an ISV has implemented the necessary controls to adopt needed compliant software.

NVIDIA's Government Ready software solves the above two issues by establishing the name Government Ready and by providing Government Ready customers with 3PAO verified software that meets the 3PAO verified standard of applicable ISV controls. NVIDIA Government Ready software should help ease an organization's compliance burden in adopting compliant AI software as they can be assured that the software itself was developed in a manner consistent with applicable FedRAMP High ISV cybersecurity requirements. While NVIDIA's Government Ready software is designed to meet the needs of FedRAMP High and related use cases, it can be used in commercial or other environments as well.

Under the Government Ready program, NVIDIA's security, product, and engineering teams selected the relevant subset of controls which apply to adoption of compliant software within a FedRAMP High cloud environment. FITS then verified implementation of these controls to ensure the Government Ready process produces repeatable, compliant software aimed at Government, Regulated Industry, and related customers alike. Related frameworks, such as GovRAMP High, share the same controls as the FedRAMP High baseline. The controls selected also have a high degree of applicability to many other global sovereign frameworks. While FITS did not directly assess the Government Ready program for compliance with these other global sovereign frameworks, it is our experience that FedRAMP controls meet and

[1] https://catalog.ngc.nvidia.com/search?policy=gov_ready

exceed a majority of global regulated / sovereign framework control needs. The control selection and summary results are captured in appendix B.

FITS evaluated and confirmed that NVIDIA's Government Ready selection of controls is consistent with federal requirements for software development. FITS then evaluated NVIDIA's methodology for enforcing that software produced under the Government Ready program meets the requirements of each selected control. FITS recognizes that while Government Ready ISV controls support adoption when incorporating software in a regulated environment, the organization deploying the software still bears a shared responsibility for integrating the software into their SDLC process, deploying, hosting, and managing the software in alignment with their requirements, and ensuring that the rest of the AI software stack similarly meets required controls for that deployment.

As a result of its 3PAO assessment the evidence that FITS reviewed provided us with a high degree of confidence that all software bearing NVIDIA's Government Ready label is produced in a manner that is consistent with the controls selected for the program and is suitable for use in the aforementioned federal, state, local and equivalent sovereign regulated environments. Organizations using Government Ready software may leverage this assessment as independent assurance that the software was produced in a manner that aligns with the list of selected controls and is suitable for use in said regulated environments.

Sincerely,



Christopher Engel
Director of Advisory Services, First Information Technology Services

Appendix A: FITS Experience

First Information Technology Services (FITS) is a deeply experienced A2LA accredited 3rd Party Assessment Organization (3PAO) / Independent Assessment Service for the U.S. General Services Administration's (GSA's) FedRAMP program and an authorized CMMC 3rd Party Assessment Organization (C3PAO) for the Department of War (DoW) CMMC program. FITS has a 25+ year track record of helping federal, state, local, sovereign and commercial customers achieve their strategic cybersecurity compliance objectives, including in the FedRAMP and DoW SRG spaces. Since our founding in January 2000, FITS has guided federal agencies and commercial cloud service providers alike through complex compliance requirements, including sustained partnerships with several of the world's hyperscale IaaS and PaaS providers. FITS regularly performs assessments and attestations for commercial entities to ensure their practices are consistent with federal requirements.

Appendix B: Government Ready Controls and Assessment Results

The following controls are included in NVIDIA's Government Ready program and were evaluated by FITS during this assessment:

CA-05, CM-06, CM-06(01), CM-06(02), CM-08, CM-08(01), CM-08(02), CM-08(03), CM-08(04), IA-05(07), IA-07, RA-05, RA-05(02), RA-05(03), RA-05(04), RA-05(05), RA-05(11), SA-10, SA-11, SA-11(01), SA-11(02), SA-15, SA-15(03), SC-13, SI-02, SI-02(02), SI-02(03), SI-03, SI-07, SI-07(15), SR-03, SR-09, SR-09(01), SR-10, SR-11, SR-11(01), SA-04(01), SA-04(02), SA-04(05)

Assessment results are summarized within the table on the next page.

Search Terms: Tags: #FedRAMP, #GovRAMP, #DoW IL, #FIPS, #FIPS 140-3, #STIG, #ISV, #GovReady, #NVIDIA, #NVAIE, #FITS, #FIRSTINFOTECH

ID	Control Name	Result
CA-5	Plan of Action and Milestones	Met
CM-6	Configuration Settings	Met
CM-6 (1)	Configuration Settings | Automated Management, Application, and Verification	Met
CM-6 (2)	Configuration Settings | Respond to Unauthorized Changes	Met
CM-8	System Component Inventory	Met
CM-8 (1)	System Component Inventory | Updates During Installation and Removal	Met
CM-8 (2)	System Component Inventory | Automated Maintenance	Met
CM-8 (3)	System Component Inventory | Automated Unauthorized Component Detection	Met
CM-8 (4)	System Component Inventory | Accountability Information	Met
IA-5 (7)	Authenticator Management | No Embedded Unencrypted Static Authenticators	Met
IA-7	Cryptographic Module Authentication	Met
RA-5	Vulnerability Monitoring and Scanning	Met
RA-5 (2)	Vulnerability Monitoring and Scanning | Update Vulnerabilities to Be Scanned	Met
RA-5 (3)	Vulnerability Monitoring and Scanning | Breadth and Depth of Coverage	Met
RA-5 (4)	Vulnerability Monitoring and Scanning | Discoverable Information	Met
RA-5 (5)	Vulnerability Monitoring and Scanning | Privileged Access	Met
RA-5 (11)	Vulnerability Monitoring and Scanning | Public Disclosure Program	Met
SA-10	Developer Configuration Management	Met
SA-11	Developer Testing and Evaluation	Met
SA-11 (1)	Developer Testing and Evaluation | Static Code Analysis	Met
SA-11 (2)	Developer Testing and Evaluation | Threat Modeling and Vulnerability Analyses	Met
SA-15	Development Process, Standards, and Tools	Met
SA-15 (3)	Development Process, Standards, and Tools | Criticality Analysis	Met
SC-13	Cryptographic Protection	Met
SI-2	Flaw Remediation	Met
SI-2 (2)	Flaw Remediation | Automated Flaw Remediation Status	Met
SI-2 (3)	Flaw Remediation | Time to Remediate Flaws and Benchmarks for Corrective Actions	Met
SI-3	Malicious Code Protection	Met
SI-7	Software, Firmware, and Information Integrity	Met
SI-7 (15)	Software, Firmware, and Information Integrity | Code Authentication	Met
SR-3	Supply Chain Controls and Processes	Met
SR-9	Tamper Resistance and Detection	Met
SR-9 (1)	Tamper Resistance and Detection | Multiple Stages of System Development Life Cycle	Met
SR-10	Inspection of Systems or Components	Met
SR-11	Component Authenticity	Met
SR-11 (1)	Component Authenticity | Anti-counterfeit Training	Met
SA-4 (1)	Acquisition Process | Functional Properties of Controls	Met
SA-4 (2)	Acquisition Process | Design and Implementation Information for Controls	Met
SA-4 (5)	Acquisition Process | System, Component, and Service Configurations	Met