Rapid7 InsightGovCloud Supplemental Terms & Conditions

By clicking 'I Agree' or otherwise indicating acceptance, including by executing an ordering document or issuing a purchase order (including through a channel partner or distributor) for the InsightGovCloud platform (the "Rapid7 Services"), the customer entity identified during the ordering or registration process ("Customer") agrees to be bound by either (1) the Government Use Addendum, if customer is a Government entity, or (2) the Rapid7 FedRAMP Addendum for Non-Federal Entities if Customer is not a Government entity (each, as applicable, the "Addendum"). The Addendum is incorporated into and forms a part of the agreement under which Customer has acquired the applicable Rapid7 Offerings (the "Subscription Agreement"). Capitalized terms not otherwise defined therein shall have the meanings ascribed to them in the Subscription Agreement.

Government Use Addendum

The parties acknowledge that the Government acquires commercial computer software under the license customarily provided to the public, to the extent such license is consistent with federal law and otherwise satisfies the Government's needs. Rapid7 agrees to modify the Subscription Agreement to remove inconsistencies with federal law and regulations as described herein solely to the extent the Customer is a Government entity. In the event of any conflict or inconsistency between this Addendum and the Subscription Agreement, this Addendum will prevail to the extent of the conflict.

1. **ADDITIONAL DEFINITIONS**

1.1 *Contract* means the Subscription Agreement as supplemented and amended by this Addendum.

1.2 *Classified Information* means (i) information designated by the U.S. government as requiring protection against unauthorized disclosure in the interest of national security (e.g., "Confidential," "Secret," or "Top Secret") under Section 1.4(a) of Executive Order 13526 or the Atomic Energy Act, or (ii) information otherwise requiring special clearance for use or access.

1.3 *Export-Controlled Information* includes any data subject to U.S. export laws including the AECA (22 U.S.C. Ch. 39), ITAR (22 C.F.R. §§ 120–130), ECRA (50 U.S.C. §§ 4801–4852), EAR (15 C.F.R. §§ 730–774), and other applicable authorities.

1.4 *Government* means any U.S. federal, state, county, or municipal agency, including independent agencies like the SEC or FCC. For this Addendum, "Government" is synonymous with "Customer."

2. **COMMERCIALITY**. The Government acknowledges that Rapid7's Services are commercial computer software developed entirely at private expense without U.S. Government funding.

3. **MODIFICATIONS TO TERMS INCONSISTENT WITH FEDERAL LAW**.

3.1 **DEFINITIONS ("Losses")**. Equitable relief, attorney's fees, costs, or interest are allowed only to the extent permitted by statute (e.g., Prompt Payment Act, Equal Access to Justice Act).

3.2 **SUBSCRIPTION FEES AND TAXES**. Any taxes allegedly due from the Government must be submitted individually to the contracting officer or included in the price.

3.3 **CONFIDENTIALITY**. Confidential information disclosures by the Government must comply with FOIA. The Government may retain confidential information as required by law or internal retention policies, provided confidentiality obligations continue.

3.4 **CUSTOMER INDEMNIFICATION**. Any Government indemnification obligation is deleted. Claims against the Government must follow the Contract Disputes Act (FAR 52.233-1). Contractor must continue performance pending resolution.

3.5 **INDEMNIFICATION PROCEDURES**. If indemnification is owed by Contractor, the Government may participate in defense at its own cost. Ultimate control lies with DOJ per 28 U.S.C. § 516.

3.6 **LIMITATION OF LIABILITY**. This does not impair the Government's rights under federal fraud statutes, including the False Claims Act (31 U.S.C. §§ 3729–3733).

3.7 **TERM**. Services tied to periodic payment (e.g., annual licenses) will not auto-renew without express Government approval from a warranted contracting officer.

3.8 **TERMINATION.** Contractor may not unilaterally revoke Government rights. Disputes must follow the Contract Disputes Act, with continued performance per FAR 52.233-1.

3.9 **FORCE MAJEURE**. Excusable delays are governed by FAR 52.249-14(f).

3.10 **GOVERNING LAW**. Disputes are governed by applicable federal law, not state or foreign laws.

3.11 **ASSIGNMENT**.. Assignment requires Government approval where restricted by the Assignment of Contracts Act (41 U.S.C. § 6305) or Assignment of Claims Act (31 U.S.C. § 3727).

4. **ADDITIONAL TERMS REQUIRED BY FEDERAL LAW**.

4.1 **END USER**. The Subscription Agreement binds the Government as end user, not individual employees in a personal capacity.

4.2 **CHANGES TO MATERIAL TERMS**. Contractor may not unilaterally revise material terms after award. Revisions must be incorporated via bilateral modification. Material terms include those that:

(a) Change Government rights/obligations;
(b) Increase Government pricing;
(c) Reduce service levels; or
(d) Limit other Government rights.

4.3 **GOVERNMENT OBLIGATIONS.** The Government will not upload or input any Classified or Export-Controlled Information into Rapid7's platform.

5. **ADDITIONAL PROVISIONS FOR FEDERAL ACQUISITION COMPLIANCE**

5.1 **APPLICABILITY**. This Section applies to all acquisitions of the Offering by or for the U.S. Federal Government, or by any prime contractor or subcontractor (at any tier) under any contract, grant, cooperative agreement, or other activity with the Federal Government for the Government's end use. The Offerings are "commercial items" as defined at FAR 2.101.

5.2 **RIGHTS IN TECHNICAL DATA AND SOFTWARE**. If the Customer is an Executive Agency (as defined in FAR 2.101) of the U.S. Federal Government:

a. Non-DoD Executive Agencies: The Government is granted only those rights in technical data and software customarily provided to Rapid7's commercial customers, pursuant to FAR 12.211 (Technical Data) and FAR 12.212 (Computer Software).
b. Executive Agencies within the Department of Defense (DoD): The Government is granted only those rights in technical data and software customarily provided to Rapid7's commercial customers, pursuant to DFARS 227.7202-3 (Rights in commercial computer software or commercial computer software documentation). In addition, DFARS 252.227-7015 (Technical Data – Commercial Items) applies to technical data provided by Rapid7.
c. GSA Schedule Contracts: Note that DFARS Subpart 227.72 does not apply to software or Offering documentation acquired under GSA schedule contracts.

5.3 **RESTRICTIONS ON ADDITIONAL RIGHTS**. Except as expressly permitted under the Subscription Agreement and this Addendum, no other rights or licenses are granted to the Government. Any additional rights requested by the Government beyond those expressly granted must be negotiated separately in writing with Rapid7.

5.4 **PRECEDENCE.** This Section supersedes any other FAR, DFARS, or other clause, provision, or supplemental regulation that addresses Government rights in the Offering, to the extent permitted by law. It operates in lieu of any inconsistent provision.

6. **OBLIGATIONS OF CUSTOMER IN FEDRAMP-AUTHORIZED ENVIRONMENT**. "FedRAMP-authorized Environment" means any information technology environment that uses one or more Rapid7 cloud services

which have obtained FedRAMP authorization, all operating within the authorized FedRAMP boundary and maintained in compliance with continuous monitoring requirements. Customer shall be solely responsible for configuring, deploying, and maintaining its use of the Rapid7 FedRAMP-authorized Environment in accordance with applicable Documentation and federal requirements. Such responsibilities include, without limitation: (i) enabling and verifying FIPS mode and any other required security configurations prior to use; (ii) recreating identity, access, and security controls in the FedRAMP-authorized Environment, including user accounts, roles, authentication methods, and keys; (iii) deploying and maintaining only FedRAMP-compliant software, agents, orchestrators, plugins, and integrations; (iv) managing its own data migration, retention, and archival, with the understanding that certain historical data and configurations cannot be transferred to the FedRAMP-authorized Environment; (v) configuring and maintaining network connectivity and firewall rules required for platform operation; and (vi) performing ongoing monitoring, reporting, and documentation necessary to maintain FedRAMP compliance. Customer acknowledges that failure to perform these responsibilities may result in degraded functionality, loss of data, or non-compliance with FedRAMP, and Rapid7 shall bear no responsibility or liability for any such failure.

6.1 **PLUG IN USE RESTRICTIONS IN FEDRAMP-AUTHORIZED ENVIRONMENT**. FedRAMP Customer shall only use plugins that are (i) included as part of the native Rapid7 product suite, and (ii) updated and certified by Rapid7 as compliant with FedRAMP requirements. No other plugins, including custom-developed or third-party plugins, may be installed, enabled, or used within the FedRAMP-authorized Environment. Rapid7 does not review, validate, support, warrant, or assume responsibility for any plugin, script, or integration not natively provided as part of the Rapid7 product suite ("Non-Native Plugins"). Customer acknowledges that use of any Non-Native Plugin may introduce unvalidated code, unauthorized data flows, or security vulnerabilities that jeopardize FedRAMP compliance. **RAPID7 EXPRESSLY DISCLAIMS ANY AND ALL RESPONSIBILITY OR LIABILITY ARISING FROM OR RELATING TO THE USE, PERFORMANCE, OR SECURITY OF NON-NATIVE PLUGINS. CUSTOMER'S USE OF ANY NON-NATIVE PLUGIN SHALL BE AT CUSTOMER'S SOLE RISK.** Customer is solely responsible for the development, deployment, maintenance, security, and operation of any Non-Native Plugin, and for any resulting operational or security impacts. Customer shall indemnify, defend, and hold harmless Rapid7 from and against any claims, damages, liabilities, costs, or expenses arising from Customer's use of Non-Native Plugins.

RAPID7 FEDRAMP ADDENDUM FOR NON-FEDERAL ENTITIES

The Federal Information Security Management Act of 2002 and the Federal Information Security Modernization Act 2014 (collectively "**FISMA**") requires each government agency to develop, document, and implement programs to provide information security for the information and information systems that support the operations and assets of the agency. To address the needs of United States ("US") Federal, State, Local and Tribal Governments along with regulated organizations that have a requirement to meet US Federal Government security standards, Rapid7 offers certain software applications and related services, including but not limited to InsightVM, InsightCloudSec and InsightConnect provisioned in a FedRAMP Moderate authorized environment (the "InsightGovCloud Platform"). Any FedRAMP customer organization other than US Federal Government entities or instrumentalities must demonstrate they have a requirement to meet US Federal Government security standards by contractually agreeing to the terms in this Addendum.

A Federal Risk Authorization Management Program ("**FedRAMP**") accredited Third Party Assessment Organization engaged by Rapid7 performed a security control assessment of the InsightGovCloud Platform at the FIPS 199 Moderate impact level in accordance with OMB Circular A-130, NIST Special Publication (SP) 800-37, and the FedRAMP Security Authorization Process. After review of the sponsoring US Federal Government agency's Authorization to Operate ("**ATO**") package for the InsightGovCloud Platform, the FedRAMP Program Management Office deemed the residual risk to government operations, data, and assets resulting from the operation of the InsightGovCloud Platform to be acceptable, and accordingly issued to Rapid7 a FedRAMP authorization at the Moderate impact level for the InsightGovCloud Platform for the benefit of Rapid7's FedRAMP customers (the "**Security Authorization**"). During the term of the Agreement, Rapid7 shall (subject to FedRAMP Customer's compliance with this Addendum) maintain such Security Authorization. The conditions for maintaining the Security Authorization to operate the InsightGovCloud Platform require the physical and logical restriction of the storage of data to hardware dedicated exclusively to InsightGovCloud Platform customers. Due to these heightened compliance requirements, certain features of the InsightGovCloud Platform may not be available to be used across InsightGovCloud Platform and non-InsightGovCloud Platform environments. Further, access to the InsightGovCloud Platform must be restricted to individuals that are US Persons, as defined under 22 CFR part 120.14, lawful permanent resident as defined in 8 USC 1101(a)(20) and protected individuals as defined in 8 USC 1324 (b) (2) ("**Approved Personnel**"), and each US FedRAMP customer accessing or using the InsightGovCloud Platform must comply with this Addendum.

1. **FedRAMP CUSTOMER RESPONSIBILITIES.** FedRAMP Customer shall: (a) restrict access to the InsightGovCloud Platform exclusively to Approved Personnel and use to its Federal accounts; (b) operate instances in the InsightGovCloud Platform that are discrete and separate from any and all instances of the offering accessible to FedRamp Customer that are not included in InsightGovCloud Platform; (c) cooperate with Rapid7 to remediate any security vulnerabilities when told to do so by Rapid7 and Rapid7 may suspend access to the InsightGovCloud Platform for security reasons at its discretion (c) promptly notify Rapid7 by email to notices@rapid7.com in the event that any of the terms of this Addendum are breached; (d) provide Rapid7 the contact information for an Information System Security Officer, or equivalent, designated by the FedRAMP Customer; (e) have and maintain an internal acceptable use policy for the InsightGovCloud Platform and a plan to communicate such policy to its employees, contractors and agents as needed to ensure compliance; and (f) provide evidence of FedRAMP Customer's compliance with this Addendum upon Rapid7's reasonable written request.

2. **COMPLIANCE**. FedRAMP Customer represents and warrants that: (a) it will comply with the terms of this Addendum, (b) it will comply with the applicable obligations set forth in both the "FedRAMP Low or Moderate Control Implementation Summary (CIS) Worksheet" and the "FedRAMP Low or Moderate Customer Responsibility Matrix (CRM) Worksheet" provided by Rapid7, (c) as an entity, it is a US Person, (d) if required by the International Traffic in Arms Regulations ("**ITAR**"), it has and will maintain a valid Directorate of Defense Trade Controls registration; (e) it is not subject to export control restrictions under US export control laws and regulations (i.e., FedRAMP Customer is not a denied or debarred party or otherwise subject to sanctions); (f) it maintains an effective compliance program to ensure compliance with applicable US export control laws and regulations, including ITAR, as applicable, and and (g) it has a requirement to comply with one or more of the below laws, regulations, rules, or data standards, (collectively, "**Protection Frameworks**"), as applicable, while operating in the InsightGovCloud Platform. The inclusion of a particular Protection Framework on the list below is not a representation that the InsightGovCloud Platform is compliant therewith. FedRAMP Customer further acknowledges that its non-compliance with the provisions of this Section 2 may result in it being a non-compliant tenant of the InsightGovCloud Platform.

Protection Frameworks

- FISMA
- FedRAMP (up to FedRAMP Moderate)
- Department of Defense Security Requirements Guide (up to DoD Impact Level 2)
- NIST SP 800-53
- OMB Circular A-130

- NIST SP 800-37
- International Traffic in Arms (ITAR)
- Covered Defense Information
- Controlled Unclassified Information (CUI)
- Criminal Justice Information (CJI)
- North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP)
- Requirements imposed on organizations from U.S. Federal government agencies (i.e., Department of Homeland Security, Department of the Treasury, Office of the Comptroller of the Currency, Centers for Medicare and Medicaid Services, etc.)

3. **OBLIGATIONS OF CUSTOMER IN FEDRAMP-AUTHORIZED ENVIRONMENT**. "FedRAMP-authorized Environment" means any information technology environment that uses one or more Rapid7 cloud services which have obtained FedRAMP authorization, all operating within the authorized FedRAMP boundary and maintained in compliance with continuous monitoring requirements. FedRAMP Customer shall be solely responsible for configuring, deploying, and maintaining its use of the Rapid7 FedRAMP-authorized Environment in accordance with applicable Documentation and federal requirements. Such responsibilities include, without limitation: (i) enabling and verifying FIPS mode and any other required security configurations prior to use; (ii) recreating identity, access, and security controls in the FedRAMP-authorized Environment, including user accounts, roles, authentication methods, and keys; (iii) deploying and maintaining only FedRAMP-compliant software, agents, orchestrators, plugins, and integrations; (iv) managing its own data migration, retention, and archival, with the understanding that certain historical data and configurations cannot be transferred to the FedRAMP-authorized Environment; (v) configuring and maintaining network connectivity and firewall rules required for platform operation; and (vi) performing ongoing monitoring, reporting, and documentation necessary to maintain FedRAMP compliance. Customer acknowledges that failure to perform these responsibilities may result in degraded functionality, loss of data, or non-compliance with FedRAMP, and Rapid7 shall bear no responsibility or liability for any such failure.

4. **PLUG IN USE RESTRICTIONS IN FEDRAMP-AUTHORIZED ENVIRONMENT**. FedRAMP Customer shall only use plugins that are (i) included as part of the native Rapid7 product suite, and (ii) updated and certified by Rapid7 as compliant with FedRAMP requirements. No other plugins, including custom-developed or third-party plugins, may be installed, enabled, or used within the FedRAMP-authorized Environment. Rapid7 does not review, validate, support, warrant, or assume responsibility for any plugin, script, or integration not natively provided as part of the Rapid7 product suite ("Non-Native Plugins"). Customer acknowledges that use of any Non-Native Plugin may introduce unvalidated code, unauthorized data flows, or security vulnerabilities that jeopardize FedRAMP compliance. **RAPID7 EXPRESSLY DISCLAIMS ANY AND ALL RESPONSIBILITY OR LIABILITY ARISING FROM OR RELATING TO THE USE, PERFORMANCE, OR SECURITY OF NON-NATIVE PLUGINS. CUSTOMER'S USE OF ANY NON-NATIVE PLUGIN SHALL BE AT CUSTOMER'S SOLE RISK.** Customer is solely responsible for the development, deployment, maintenance, security, and operation of any Non-Native Plugin, and for any resulting operational or security impacts. Customer shall indemnify, defend, and hold harmless Rapid7 from and against any claims, damages, liabilities, costs, or expenses arising from Customer's use of Non-Native Plugins.