Service Description - SecurID® Cloud Service

*** IMPORTANT INFORMATION – PLEASE READ CAREFULLY ***

The use of the SecurID® Cloud Service described herein is subject to and expressly conditioned upon acceptance of the: (i) Terms of Service between RSA and Customer or, if the parties have no such agreement in place, the Terms of Service for SecurID® Cloud Offerings currently located at https://www.rsa.com/en-us/company/standard-form-agreements (the "Terms of Service"); (ii) the Data Processing Addendum for SecurID Cloud Offerings located at https://www.rsa.com/en-us/company/standard-form-agreements (the "DPA), and (iii) the applicable ordering document covering Customer's purchase of a subscription or subscriptions to the SecurID Cloud Service from RSA or an RSA authorized reseller, the terms of which are incorporated herein by reference (such Terms of Service, DPA, ordering document, and this Service Description are, collectively, the "Agreement").

This Service Description is a legally binding document between you (meaning the individual person or the entity that the individual represents that is purchasing subscriptions to the SecurID Cloud Service for its internal use and not for outright resale ("Customer")) and RSA (which means (i) RSA Security LLC, if Customer is located in the United States, Mexico or South America; (ii) the local RSA sales subsidiary if Customer is located outside United States, Mexico or South America and in a country in which RSA has a local sales subsidiary; (iii) the local Dell Technologies ("Dell") or EMC Corporation ("EMC") entity authorized by RSA on the RSA quote or other RSA ordering document, if Customer is located outside United States, Mexico or South America and in a country in which RSA does not have a local sales subsidiary; or (iv) RSA Security & Risk Ireland Limited or other authorized RSA entity as identified on the RSA quote or other RSA ordering document if Customer is located in a country in which neither RSA Security LLC nor Dell or EMC has a local sales subsidiary). Unless RSA agrees otherwise in writing, this Service Description and the Agreement governs Customer's use of the SecurID Cloud Service except to the extent all or any portion of the SecurID Cloud Service is subject to a separate written agreement set forth in a quotation issued by RSA.

By proceeding with the use of the SecurID Cloud Service or authorizing any other person to do so, you are representing to RSA that you are (i) authorized to bind the Customer; and (ii) agreeing on behalf of the Customer that the terms of the Agreement shall govern the relationship of the parties with regard to the subject matter of the Agreement and are waiving any rights, to the maximum extent permitted by applicable law, to any claim anywhere in the world concerning the enforceability or validity of the Agreement. If you do not have authority to agree to the terms of this Service Description or the Agreement on behalf of the Customer, or do not accept the terms of this Service Description on behalf of the Customer, immediately cease any further attempt to use the SecurID Cloud Service for any purpose.

This Service Description governs the provision by RSA of the RSA cloud offering known as "SecurID Cloud Service" to which Customer has purchased a valid subscription therefore. Notwithstanding anything to the contrary in the Agreement, in the event of a conflict between the Terms of Service and/or ordering document and this Service Description, the terms of this Service Description shall prevail solely with respect to the subject matter hereof. Capitalized words used in this Service Description and not expressly defined herein will have the meaning stated in the Agreement.

Service levels and operational procedures are standardized for all customers.

1. SCOPE OF SERVICES.

During the term of Customer's subscription to the SecurID Cloud Service as set forth in the ordering document (the "**Term**"), RSA will provide Customer with access to and use of the SecurID Cloud Service (the "**Service Offering**") via the internet in accordance with the service levels set forth in Exhibit 1 hereof and as further described therein. Customer's access and use of the Service Offering will be subject to all those restrictions stated in the Agreement.

2. SERVICE OFFERING.

The Service Offering provides a multi-tenant, cloud-hosted platform for access and authentication that provides Customer with the ability to control how users access resources with centralized access and authentication policies. The Service Offering is designed to protect SaaS and on-premise web applications, third party single sign-on (SSO) solutions, and on-premises resources. The Service Offering is offered in several package levels. Customer's accepted order for the Service Offering will state which package has been selected by Customer.

Incidental Software provided with the Service Offering is governed by the End User License Agreement located at https://www.rsa.com/content/dam/en/terms/eula-shrinkwrap.pdf. Incidental Software will be listed on the applicable ordering document and may include, but is not limited to, the RSA Identity Router software.

3. ACCOUNT ACCESS.

RSA will deliver to Customer an application administrator user ID, password, and other account information ("**Account Access Information**") necessary for Customer to access the Service Offering in accordance with the Agreement. Thereafter, Customer will create and manage Account Access Information for each authorized user of the Service Offering. Customer is responsible for all activity occurring under such Account Access Information and shall abide by all applicable local, state, national, and foreign laws, treaties, and regulations ("**Applicable Laws**") in connection with Customer's use of the Service Offering, including but not limited to those related to data privacy, international communications, and the transmission of technical or personal data.

4. CUSTOMER RESPONSIBILITIES.

Customer will provide RSA with the cooperation, access, and detailed information reasonably necessary for RSA to implement and deliver the Service Offering, including, where applicable, one (1) employee who has substantial computer system, network management, and project management experience satisfactory to RSA to act as project manager and as a liaison between RSA and Customer. RSA will be excused from its failure to perform any obligation under this Service Description to the extent such failure is caused by Customer's delay or failure to perform its responsibilities under this Agreement. Customer shall use reasonable and appropriate safeguards to protect its Customer Attributes (as defined below).

5. CUSTOMER ATTRIBUTES.

RSA requires access to only the following end user attributes from the Customer (collectively, "**Customer Attributes**") in order to provide the Service Offering to Customer: First Name, Last Name, Email Address, Username, Primary Unique Identifier (entryDN), Secondary Unique Identifier (GUID), Account Status, and Account Expiration. No other personally identifiable information is required in order for the Customer to access or use the Service Offering, including but not limited to, any personally identifiable information that is "sensitive" by nature or deemed "sensitive" by any Applicable Laws (such as social

security numbers, credit card data, drivers' license numbers, national ID numbers, bank account numbers, and health/medical information) (collectively, "**Sensitive PII**"). During the Term, Customer grants to RSA a limited, non-exclusive license to use the Customer Attributes solely for all reasonable and necessary purposes contemplated by this Service Description and for RSA to provide the Service Offering. Customer, not RSA, shall have sole responsibility for the accuracy, quality, integrity, legality, reliability, appropriateness and intellectual property ownership or right to use of all Customer Attributes. RSA shall use reasonable and appropriate administrative, technical and physical safeguards to protect the security, integrity and confidentiality of the Customer Attributes. However, for clarity, Customer acknowledges and agrees that 1) the Service Offering is not intended or designed to securely host and store any Sensitive PII, and 2) Customer shall not modify or use the Service Offering to store any such Sensitive PII or provide RSA with access to any Sensitive PII or information other than the Customer Attributes.

6. RSA OBLIGATIONS.

A. General.

RSA will, through its cloud infrastructure provider, supply and maintain adequate heating/cooling; electrical power; server hardware; network infrastructure and bandwidth; physical security and access controls; and professional fire detection/suppression capability necessary to provide the Service Offering.

B. Application Upgrades.

During the Term, RSA reserves the right to make modifications, including upgrades, patches, revisions or additions to the Service Offering subject to the terms set forth in Exhibit 1.

C. Malware Protection.

RSA will install and run industry standard malware protection on all systems underlying the Service Offering. Anti-malware definition files shall be updated regularly in accordance with industry standards. For the avoidance of doubt, Customer remains responsible for protecting its own systems by installing, updating, and maintaining industry standard malware protection.

D. Logging.

RSA will monitor and log all authentication and administrative system access to the Service Offering and will maintain at least thirty (30) day backups of such logs. Such logs are RSA Confidential Information, but will be disclosed as necessary to comply with Applicable Law and to Customer upon written request.

EXHIBIT 1

SecurID Cloud Service - SERVICE LEVELS

I. SERVICE LEVELS FOR PRODUCTION INSTANCE.

This Section I of Exhibit 1 applies to Customer's Production Instance of the Service Offering. For purposes of this Exhibit 1, "**Production Instance**" means solely Customer's production instance of the Service Offering's cloud computing environment used solely for authentication activities. The Production Instance shall have 99.95% or higher Availability on a monthly basis (the "**Production Availability Standard**"), calculated as set forth below. "**Availability**" means, subject to the exclusions below, solely the availability of the cloud authentication components of the Service Offering and does not apply to any components of the Service Offering that are not delivered by RSA over the internet as part of the Service Offering (e.g., Incidental Software) or other RSA products, software, services, solutions, maintenance, or support services.

A. PRODUCTION INSTANCE INTERRUPTIONS.

1. **Measurement.** Production Downtime, as defined below, is measured from the RSA-confirmed commencement time of a Production Downtime event to the time the Production Instance is operational.

2. **Exclusions.** Unavailability of the Production Instance shall not be considered Production Downtime to the extent that it is caused by one or more of the following factors:

   (i) Customer's failure to perform any of its obligations under the Agreement;

   (ii) Issues with or lack of network connectivity between the IT systems of Customer to the Service Offering;

   (iii) The written request or consent by Customer's representative to interrupt the Production Instance; and

   (iv) Force Majeure Events which shall mean strikes, riots, insurrection, terrorism, fires, natural disasters, acts of God, war, governmental action, pandemics, epidemics, or any other cause which is beyond the reasonable control of RSA.

   RSA shall be solely responsible for establishing the extent to which Production Downtime is caused by one or more of the above factors.

B. PRODUCTION INSTANCE SERVICE LEVEL STANDARD AND MEASUREMENT.

1. **General.** Availability for each elapsed calendar month is calculated as follows:

   M = total number of minutes in the elapsed calendar month;
   Y = actual total minutes of emergency or unscheduled maintenance which shall not exceed 240 minutes per month;
   N = actual authorized Availability in minutes for the elapsed month which is calculated as follows:

N = [(M – Y) x 99.95%]

X = the number of minutes the Production Instance is authorized to not be available in the elapsed month and which is calculated as follows:
X = M - N

D = the number of minutes in the elapsed month that the Production Instance is not available ("**Production Downtime**").

If D > X Customer will qualify for a service credit as follows.

If RSA fails to meet the Production Availability Standard in any two months within a three month rolling period (commencing from the month where the Production Availability Standard first failed), then RSA shall issue to the Customer a service credit (a "**Service Level Credit**") in an amount equal to the percentage by which RSA missed the Production Availability Standard of the total fees received for the Service Offering for each of the months during which such failures were measured. However, notwithstanding the foregoing, in no event shall Service Level Credits exceed five percent (5%) of the total Fees received for the Service Offering for such months. The Customer must request a Service Level Credit from RSA in the event that a Service Level Credit is due. The remedies specified in this Section I.B.1. shall be the Customer's sole and exclusive remedies for the failure of RSA to meet the Production Availability Standard.

2. **Credit Request and Payment Procedures.** To receive a Service Level Credit, Customer (for logging/tracking purposes) must make a request by sending an email to SecurID.Service.Credit.Request@rsa.com. Each request in connection with this Section I.B. must include the dates and times of the failure to meet Production Availability Standard and must be received by RSA within five (5) business days after receiving the report described under Section I.C. below. If the failure to meet Production Availability Standard is confirmed by RSA, Service Level Credits will be applied within two billing cycles after RSA's receipt of Customer's credit request. Service Level Credits are not refundable and can be used only towards future billing charges.

C. SERVICE LEVEL REPORTING.

Customer may access RSA's monthly reports of Availability at https://community.rsa.com/t5/rsa-securid-access-cloud/monitor-uptime-status-for-the-cloud-authentication-service/ta-p/571141.

D. GENERAL OBLIGATIONS.

RSA will use commercially reasonable efforts consistent with generally accepted industry standards and best practices of leading companies in the critical data storage and security industry to: (i) protect the Production Instance and supporting infrastructure controlled or maintained by RSA; (ii) monitor the Production Instance and supporting infrastructure controlled or maintained by RSA for problems; (iii) identify root causes; (iv) correct problems; and (v) minimize recurrences of missed Availability for which it is responsible. Should a Force Majeure Event result in unavailability of the Service Offering, RSA will focus its efforts on restoring availability of the Service Offering first to the Production Instance, and then to the Non-Production Instance.

II. NON-PRODUCTION INSTANCE.

This Section II of Exhibit 1 applies, if applicable, to Customer's Non-Production Instance of the Service Offering. "**Non-Production Instance**" means the computing environment, applications, and security associated with the Service Offering allocated by RSA for customers to access and use in execution of

their business development and/or testing processes. A Non-Production Instance is only provided to Customer upon Customer's written request to RSA. Customer acknowledges that Service Offering in the Non-Production Instance are at-risk services given that they are in support of Customer development, user acceptance testing, pre-production staging, and preview(s) of upcoming Service Offering changes to the Production Instance. As such, the Service Offering provided in the Non-Production Instance is not subject to any availability standard and is not eligible for credits on future charges as a result of failure to meet or exceed the Production Availability Standard for the Production Instance.

EXHIBIT 2

INFORMATION SECURITY AND BUSINESS CONTINUITY PLANNING FOR SECURID CLOUD SERVICE

I. ADHERENCE TO STANDARDS OF PROTECTION.

RSA will apply commercially reasonable efforts to carry out the procedures set forth in this Exhibit 2 to protect the Production Instance. In fulfilling its obligations under this Exhibit 2, RSA may, from time to time, use methods or procedures ("**Processes**") similar to and substantially conforming to certain terms herein. RSA shall ensure that any such Processes are no less rigorous in their protection to Customer than the standards reflected in this Exhibit's terms set forth below and shall provide safeguards no less protective in all material respects than those in this Exhibit 2.

A. Definitions.

1. **"Authorized Persons"** means RSA's employees, contractors, or other agents who need to access Customer Attributes to enable RSA to perform its obligations under the Agreement, and who are bound by confidentiality and other obligations sufficient to protect Customer Attributes in accordance with the terms and conditions of the Agreement.

2. **"Encryption"** is a process of using an algorithm to transform data into coded information in order to protect confidentiality.

3. **"Firewall"** is an integrated collection of security measures used to prevent unauthorized electronic access to a networked computer system.

4. **"Intrusion Detection Process"** (or "**IDP**") is a method of reviewing system events and Processes in near real time and, without unreasonable delay, alerting management to known patterns of behavior that indicate an intrusion is occurring or is likely to take place soon.

5. **"Security Incident"** means any loss of, or unauthorized or unlawful access to, acquisition of, use of, or disclosure of, Customer Attributes within the possession (e.g., the physical or IT environment) of RSA or any Authorized Person.

B. Breach Notification and Remediation.

In the event RSA becomes aware of a Security Incident, RSA shall, in the most expedient time possible under the circumstances, notify Customer of the Security Incident and shall, subject to Applicable Laws or a governmental request, provide Customer with details to the extent available about the Security Incident, including how it occurred and how RSA will address the Security Incident. In the event of a Security Incident, RSA and Customer shall cooperate in good faith to resolve any privacy or data security issues involving Customer Attributes, and to make any legally required notifications to individuals affected by the Security Incident. In the event of an actual Security Incident involving RSA's systems or network, RSA shall:

1. **Breach Notification.** Within seventy-two (72) hours after becoming aware of the Security Incident, notify Customer of the approximate date and time of the Security Incident and a summary of known, relevant facts and actions taken to rectify the Processes and address the

Security Incident's effects.

2. **Breach Remediation.** Promptly implement reasonable measures necessary to address the security of RSA's systems and the security of Customer Attributes. If such measures include temporarily restricting access to any information, network, or systems comprising the Service Offering in order to mitigate against further breaches, RSA shall promptly notify Customer of the restricted access, in advance of such restriction when possible but in all cases as soon as possible under the circumstances. RSA shall cooperate in good faith with Customer to allow Customer to verify RSA's compliance with its obligations under this clause.

C. Independent Control Attestation and Testing.

RSA shall employ independent third party oversight as follows:

1. **Attestation.** At least annually and at its own expense, RSA shall ensure that an audit of the hosted environment where Customer Attributes are stored, processed, or transmitted by RSA is conducted according to appropriate industry security standards by an independent third party auditor and that such audit will result in the generation of an industry standard audit report (for example, SSAE-18 SOC 2, Type II, ISO 27001, or similar) ("**Audit Report**"). Customer may request a copy of the most recent Audit Report from RSA in writing no more than once annually.

2. **Penetration Testing.** At least annually and at its own expense, RSA shall engage a third party testing service provider for network penetration testing of the RSA infrastructure and systems used to provide the Service Offering. Customer may request a copy of the executive summary of the most recent penetration testing report from RSA in writing no more than once annually.

D. Data Security. RSA shall use commercially reasonable efforts to carry out the following procedures to manage Customer Attributes as follows:

1. **Information Classification.** If Customer discloses Customer Attributes to Service Provider or if Service Provider accesses Customer Attributes as permitted by the Agreement, Customer Attributes shall be classified as Confidential Information and handled in accordance with the terms hereof.

2. **Encryption of Information.** Industry-standard encryption techniques (for example, public encryption algorithms such as, RC5, IDEA, RSA and AES) shall be used at cipher strengths no less than 256-bit or equivalent for Customer Attributes. RSA shall use industry standard authentication practices to authenticate parties and secure messages and/or communications involving Customer Attributes.

3. **Cryptographic Key Management.** RSA shall ensure that cryptographic keys are managed securely in accordance with control requirements and procedures which are consistent with industry best practices, and shall ensure that Customer Attributes are protected against unauthorized access or destruction. RSA shall ensure that if public key infrastructure (PKI) is used, it shall be protected by 'hardening' the underlying operating system(s) and restricting access to certification authorities.

4. **Data Access; Transmission.** RSA shall make RSA-controlled applications and systems used to process or store Customer Attributes accessible only by those whose job responsibilities require such access. If transferred across the Internet, wireless network (e.g., cellular, 802.11x, or similar technology), or other public or shared networks, Customer Attributes shall be protected using

appropriate cryptography.

5. **Event Logging.** For systems directly providing the Service Offering to Customer, RSA shall maintain logs of key events that may affect the confidentiality, integrity, and/or availability of the Service Offering to Customer and that may assist in the identification or investigation of material incidents and/or security breaches occurring in relation to RSA systems. The logs shall be retained for at least 30 days and protected against unauthorized changes (including, amending or deleting a log).

6. **Removable Media.** "**Removable Media**" means portable or removable magnetic and/or optical media, including but not limited to hard disks, floppy disks, USB memory drives, zip disks, optical disks, CDs, DVDs, digital film, memory cards, magnetic tape, and other removable data storage media whether owned by Customer or RSA. The use of Removable Media is prohibited unless authorized by Customer in writing.

7. **Media Disposal and Servicing.** In the event that functional storage media used in connection with the Service Offering must be disposed of or transported for servicing, RSA shall ensure Customer Attributes are not accessible from such media. Non-functional media shall be aggregated in a secure area until enough of it exists to warrant destruction by a contracted, bonded third party of RSA's choosing, and a certificate of destruction shall be supplied to RSA by such third party promptly upon its destruction.

E. Computer & Network Security. RSA shall use commercially reasonable efforts to carry out the following procedures to protect Customer Attributes:

1. **Server Security.** Computer systems comprising the Service Offering shall be dedicated solely to the provision of the Service Offering and not used by RSA for development and/or testing unless required to fulfill obligations within this Agreement.

2. **Internal Network Segment Security.** Data entering the Service Offering's network from external sources shall pass through Firewalls to enforce secure connections between internal and external systems.

3. **External Network Segment Security.** The Service Offering's connections to the Internet shall (a) have appropriate security measures and controls applied, and (b) include an IDP that monitors data within the external network segment and information coming to Firewalls. RSA's IDP shall be designed to detect and report unauthorized activity prior to entering the Firewalls. RSA shall disable unnecessary network access points.

4. **Network and Systems Monitoring.** RSA shall actively monitor its networks and systems used to provide the Service Offering to detect deviation from access control policies and actual or attempted intrusions or other unauthorized acts.

5. **User Authentication.** RSA shall implement Processes designed to authenticate the identity of its system users through the following means:

    a) User IDs. Each user of a system containing Customer Attributes shall be assigned a unique identification code ("**User ID**").

    b) Passwords. Each user of a system containing Customer Attributes shall use a unique password whose length, complexity, and age should be governed in accordance with

industry best practices.

c) Two-Factor Authentication for Remote Access. Remote access to systems containing Customer Attributes shall require the use of two-factor authentication.

d) Deactivation. RSA User IDs shall be automatically deactivated after a technologically enforced number of unsuccessful log-in attempts. Interactive sessions shall be restricted or timed out after a technologically enforced period of inactivity. User IDs for RSA Personnel with access to Customer Attributes shall be deactivated promptly upon changes in job responsibilities that render such access unnecessary and during termination of employment.

6. **Account Access.** RSA shall provide account access to RSA Personnel on a least-privilege, need to know basis.

F. System Development.

1. **Development Methodology and Installation Process.**

a) Documented Development Methodology. RSA shall ensure that development activities for RSA- developed software used in the provision of the Service Offering are carried out in accordance with a documented system development methodology.

b) Documented Deployment Process. RSA shall ensure that new systems and changes to existing systems used in the provision of the Service Offering are deployed in accordance with a documented process.

2. **Testing Process.** RSA shall ensure that all reasonable elements of a system (e.g., application software packages, system software, hardware and services) shall be tested at all relevant stages of the systems development lifecycle before applicable system changes are promoted to the production Instance.

3. **Customer Attributes in Test Environments.** RSA shall ensure that Customer Attributes are not used within RSA test environments without Customer's prior written approval.

4. **Secure Coding Practices.** RSA shall have secure development practices for itself and require the same of its subcontractors, including the definition, testing, deployment, and review of security requirements.

G. General Security.

1. **Point of Contact.** RSA shall designate an account manager with whom Customer may coordinate as an escalation point beyond typical Service Offering customer support avenues available to Customer.

2. **Cloud Hosting Facilities.** RSA shall ensure that the cloud provider(s) RSA engages to host the Service Offering use industry best standards for physical security of their data centers such as barrier access controls (e.g., the use of guards and entry badges) that provide a physical environment secure from unauthorized access, damage, and interference.

Additional requirements specific to Authorized Persons' access to the Service Offering are:

a) Two-Factor Authentication. Two-factor authentication shall be required for any access to the Service Offering; and

b) Limited Internet Access. Authorized Persons shall have access to external email and/or the Internet from within the Service Offering environment only to the extent required by job function in support of the Service Offering.

3. Change and Patch Management. RSA shall use commercially reasonable efforts to ensure that changes (including but not limited to emergency fixes, application patches, firmware updates, and similar) to its applications and infrastructure associated with the Service Offering are tested, reviewed, approved, and applied using an industry standard change management process that accounts for risks to RSA, its customers, and other such factors as RSA deems relevant.

4. RSA Personnel.

a) Background Screening. RSA shall perform background checks in accordance with RSA screening policies on all RSA employees and consultants who are or will be supporting the Service Offering under this Agreement, to the extent permitted by Applicable Law.

b) Training. RSA personnel involved in the provision of the Service Offering shall receive appropriate ongoing security awareness training. Such security awareness training shall be provided to RSA personnel being engaged in the provision of the Service Offering or prior to RSA personnel being given access to Customer Attributes.

II. CONTINUITY AND DIASTER RECOVERY PLANNING.

RSA shall ensure that the Service Offering disaster recovery and continuity of operations contingency policies and procedures are in place that to facilitate the implementation of the contingency planning associated policies and controls for the Service Offering necessary to perform RSA's obligations under this Agreement. RSA shall:

1. require a remote contingency site with adequate security and capacity to provide the Service Offering in accordance with the obligations of this Agreement;

2. require Processes designed to ensure that Customer Attributes and other data necessary for the performance of the Service Offering are automatically copied to a remote contingency site;

3. include a description of the recovery process to be implemented following the occurrence of a disaster;

4. detail key Processes, personnel, resources, services and actions necessary to ensure that Service Offering continuity is maintained;

5. include a twelve (12) hour recovery time objective ("**RTO**") in which the Service Offering shall be recovered following notification that disaster recovery event is declared ; and

6. allow for the recovery of Customer Attributes at the remote contingency site in accordance with a three (3) hour recovery point objective ("**RPO**").

B. Testing. At least annually and at its own expense, RSA will perform disaster recovery, continuity of operations assessments. Upon reasonable request, RSA will provide an overview consisting of the

date(s), scope, and outcome (on a succeed or fail basis) of the last test.

C. **Notification.** In case of a Force Majeure Event that RSA reasonably believes will impact the Service Offering or its ability to perform its obligations under this Agreement, RSA shall, to the extent possible, promptly notify Customer of such Force Majeure Event via RSA's notification system located at https://status.securid.com/. Such notification shall, as soon as such details are known, contain:

1. a description of the Force Majeure Event in question;
2. the impact the Force Majeure Event is likely to have on the Service Offering and RSA's obligations under this Agreement;
3. the operating strategy and the timetable for the utilization of the contingency site; and
4. the timeframe in which RSA expects to return to business as usual.