۵۹۷۵۸/۵۳۸۴۳

۱۴۰۱/۴/۵

جمهوری اسلامی ایران

رئیس جمهور

بسمه تعالی

"با صلوات بر محمد و آل محمد"

جناب آقای دکتر قالیباف

رییس محترم مجلس شورای اسلامی

لایحه "موافقت‌نامه همکاری در حوزه امنیت اطلاعات بین دولت جمهوری اسلامی ایران و دولت فدراسیون روسیه" که به پیشنهاد وزارت امور خارجه در جلسه ۱۴۰۱/۲/۲۵ هیئت وزیران به تصویب رسیده است، برای انجام تشریفات قانونی به پیوست تقدیم می‌شود.

سید ابراهیم رئیسی

رییس جمهور

۵۹۷۵۸/ ۵۳۸۲۲
۱۴۰۱/۴/۵

جمهوری اسلامی ایران
رئیس جمهور

بسمه تعالی

مقدمه توجیهی:

با توجه به وجود تهدیداتی مانند نقض حاکمیت، امنیت و تمامیت ارضی کشورها، وارد کردن خسارات اقتصادی به تأسیسات زیرساخت‌های مربوط به اطلاعات، دسترسی غیرمجاز به اطلاعات رایانه‌ای، انتشار اطلاعات زیان‌بار برای نظام‌های اجتماعی – سیاسی و محیط معنوی، اخلاقی و فرهنگی دولت‌ها و ضرورت همکاری دولت‌های جمهوری اسلامی ایران و فدراسیون روسیه درخصوص مبارزه با تهدیدات یادشده و تقویت امنیت اطلاعات، مبارزه با جرایم ارتکابی در حوزه استفاده از فناوری‌های اطلاعات و ارتباطات، کمک‌های فنی و فناوری و همکاری بین‌المللی، لایحه زیر برای تشریفات قانونی تقدیم می‌شود:

لایحه موافقت‌نامه همکاری در حوزه امنیت اطلاعات بین دولت جمهوری اسلامی ایران و دولت فدراسیون روسیه

ماده واحده – موافقتنامه همکاری در حوزه امنیت اطلاعات بین دولت جمهوری اسلامی ایران و دولت فدراسیون روسیه مشتمل بر یک مقدمه، نه ماده و یک ضمیمه به شرح پیوست تصویب و اجازه مبادله اسناد آن داده می‌شود.

تبصره– اعمال بند (۲) ماده (۵)، بند (۶) ماده (۶) و بند (۲) ماده (۹) این موافقتنامه، منوط به رعایت تشریفات مندرج در اصول (۷۵) و (۱۲۵) قانون اساسی جمهوری اسلامی ایران می‌باشد.

وزیر امورخارجه

رییس جمهور

موافقت‌نامه

بین

دولت جمهوری اسلامی ایران و

دولت فدراسیون روسیه

در خصوص همکاری در حوزه امنیت اطلاعات

دولت جمهوری اسلامی ایران و دولت فدراسیون روسیه که از این پس "طرف‌ها" نامیده می‌شوند،

عطف به «معاهده اساس روابط متقابل و اصول همکاری بین دولت جمهوری اسلامی ایران و دولت فدراسیون روسیه» در ۲۲ اسفند ۱۳۷۹ (۱۲ مارس ۲۰۰۱)،

با امعان نظر به اینکه پیشرفت قابل توجهی در توسعه و به‌کارگیری جدیدترین فناوری‌های اطلاعات و ارتباطات حاصل شده است،

با امعان نظر به اهمیت فراوان فناوری‌های اطلاعات و ارتباطات برای توسعه اجتماعی و اقتصادی به نفع رفاه بشریت و حمایت از صلح، امنیت و ثبات بین‌المللی در جهان معاصر،

با ابراز نگرانی از تهدیدهای مرتبط با استفاده احتمالی از چنین فناوری‌هایی در تعارض با اهداف تضمین صلح، امنیت و ثبات بین‌المللی، با هدف تضعیف حاکمیت و امنیت کشورها و دخالت در امور داخلی آنها، نقض حریم خصوصی شهروندان، برهم زدن اوضاع سیاسی، اجتماعی و اقتصادی داخلی و بر افروختن خصومت بین اقوام و مذاهب،

با تاکید بر ضرورت حداکثرسازی منافع مشترک خود از ناحیه فناوری‌های اطلاعات و ارتباطات و کاهش تهدیدهای مشترک ناشی از آن علیه خود،

همچنین با تاکید بر ضرورت تام احترام به قوانین و مقررات دولت‌های طرف‌ها در اجرای این موافقت‌نامه،

ضمن شناسائی اهمیت فراوان امنیت اطلاعات برای نظام امنیت بین‌المللی،

با تایید اینکه حاکمیت دولت و اصول و مقررات بین‌المللی نشات گرفته از آن بر رفتار دولت‌ها در چارچوب فعالیت‌های مربوط به فناوری‌های اطلاعات و ارتباطات و بر صلاحیت قضایی کشورها نسبت به زیرساخت فناوری‌های اطلاعات و ارتباطات در خاک آنها اعمال می‌شود و همچنین با تایید اینکه دولت‌ها واجد حقوق حاکمیتی برای تعیین و اجرای سیاست خود در خصوص مسائل مرتبط با شبکه اطلاعاتی و مخابراتی اینترنت، از جمله تضمین امنیت هستند،

با اعتقاد به اینکه اعتمادسازی بیشتر و توسعه همکاری میان طرف‌ها در حوزه فناوری‌های اطلاعات و ارتباطات یک ضرورت فوری است و تامین کننده منافع آنها است،

ضمن قائل شدن اهمیت فراوان برای توازن بین تضمین امنیت و رعایت حقوق بشر در حوزه استفاده از فناوری اطلاعات و ارتباطات، منطبق با قوانین ملی و تعهدات بین‌المللی دولت‌های طرف‌ها،

ضمن تلاش برای پیشگیری و مقابله با تهدیدات متوجه امنیت اطلاعات، و تلاش برای تامین منافع امنیت اطلاعات دولت‌های طرف‌ها با هدف ایجاد یک محیط اطلاعات بین‌المللی صلح‌آمیز و امن،

با محکومیت اقدامات قهری یک جانبه اتخاذ شده در نقض منشور ملل متحد،

همچنین ضمن تلاش برای کار مشترک با هدف کاهش آسیب‌پذیری دولت‌ها در مقابل تهدیدات علیه امنیت اطلاعات، شامل تهدید اقدامات بالقوه محدودساز و مسدودساز علیه دولت‌های طرف‌ها در ارتباط با فناوری‌های اطلاعات و ارتباطات و دسترسی به اینترنت،

نیز ضمن تلاش برای همکاری نزدیک در مجامع منطقه‌ای و بین‌المللی با هدف توسعه و ارتقای هنجارها و مقررات حقوقی به‌منظور تضمین امنیت بین‌المللی اطلاعات، از جمله از طریق حکمرانی عادلانه اینترنت،

با تمایل به ایجاد چهارچوب دوجانبه برای همکاری میان دولت‌های طرف‌ها در حوزه امنیت اطلاعات،

به شرح زیر به توافق رسیدند:

ماده ۱

واژگان اصلی

۱. با هدف اجرای این موافقت‌نامه، طرف‌ها بر تعاریف واژگان اصلی مندرج در پیوست، که بخش تفکیک‌ناپذیر این موافقت‌نامه می‌باشد، توافق می‌نمایند.
۲. در صورت ضرورت، پیوست می‌تواند با توافق طرف‌ها، تکمیل، اصلاح و روزآمد شود.

ماده ۲

تهدیدات اصلی در حوزه امنیت اطلاعات

همکاری طرف‌ها به موجب این موافقت‌نامه بر این اساس استوار است که استفاده از فناوری‌های اطلاعات و ارتباطات، ازجمله با اهداف زیر، واجد تهدیدات اصلی علیه امنیت اطلاعات می‌باشد:

۱) دست زدن به اقدامات ناقض حاکمیت، امنیت و تمامیت ارضی کشورها؛

۲) وارد کردن خسارات اقتصادی و سایر خسارات از جمله تاثیر مخرب بر تاسیساتِ زیرساخت‌های حیاتی اطلاعات و سایر زیرساخت‌های مربوط به اطلاعات؛

۳) مقاصد تروریستی، از جمله تبلیغات تروریستی و استخدام افراد برای فعالیت‌های تروریستی؛

۴) ارتکاب جرایم، از جمله جرائم مرتبط با دسترسی غیرمجاز به اطلاعات رایانه‌ای؛

۵) دخالت در امور داخلی دولت‌ها، اختلال در نظم عمومی، برافروختن خصومت بین اقوام، نژادها و مذاهب، ترویج ایده‌ها و تئوری‌های نژادپرستانه و دیگرهراسی که باعث نفرت و تبعیض می‌شوند و خشونت و بی‌ثباتی را برمی‌انگیزند، و بی‌ثبات کردن اوضاع سیاسی، اجتماعی و اقتصادی داخلی و دخالت در اداره دولت؛

۶) انتشار اطلاعاتی که برای نظام‌های اجتماعی-سیاسی و اجتماعی-اقتصادی و نیز برای محیط معنوی، اخلاقی و فرهنگی دولت‌های دیگر زیانبار است.

ماده ۳

حوزه‌های اصلی همکاری دوجانبه

۱. با توجه به تهدیدات اصلی اشاره شده در ماده ۲ این موافقت‌نامه و نیاز به تضمین امنیت اطلاعات، طرف‌ها، نمایندگان مجاز و نهادهای ذیصلاح دولت‌های طرف‌هاکه طبق ماده ۵ این موافقت‌نامه تعیین می‌شوند، در خصوص موضوعاتی نظیر تقویت امنیت اطلاعات، مبارزه با جرائم ارتکاب یافته در حوزه استفاده از فناوری‌های اطلاعات و ارتباطات، کمک‌های فنی و فناوری، و همکاری بین‌المللی، از جمله در زمینه‌های کلیدی زیر همکاری خواهند نمود:

۱) شناسایی، هماهنگی و انجام همکاری لازم در مجامع منطقه‌ای و بین‌المللی برای تضمین امنیت ملی و بین‌المللی اطلاعات؛

۲) تدوین و پیشبرد قواعد حقوق بین‌الملل قابلِ اِعمال به‌منظور تضمین امنیت ملی و بین‌المللی اطلاعات؛

۳) مقابله با تهدیدات در حوزه تضمین امنیت اطلاعات مندرج در ماده ۲ این موافقت‌نامه؛

۴) تبادل اطلاعات و همکاری در حوزه اجرای قانون با هدف پیشگیری، کشف، مبارزه، تحقیق و پیگرد قضایی جرایم مرتبط با استفاده از فناوری‌های اطلاعات و ارتباطات برای اهداف تروریستی و مجرمانه؛

۵) مشارکتِ در مذاکرات چندجانبه در خصوص اقدامات اعتمادساز مربوط به امنیت بین‌المللی اطلاعات؛

۶) تبادل اطلاعات بین نهادهای ذیصلاح دولت‌های طرف‌ها در حوزه امنیت اطلاعات، شامل همکاری بین نهادهای مربوط حوزه واکنش به حوادث رایانه‌ای دولت‌های طرف‌ها؛

۷) تبادل اطلاعات درباره قوانین ملی دولت‌های طرف‌ها مرتبط با تضمین امنیت اطلاعات؛

۸) همکاری به‌منظور پرداختن به پیامدهای منفی اقدامات قهری یک جانبه ناقض منشور سازمان ملل متحد وحقوق بین‌الملل در حوزه تضمین امنیت اطلاعات؛

۹) ارتقای کیفی چارچوب حقوقی دوجانبه و سازکارهای عملی همکاری میان دولت‌های طرف‌ها با هدف تضمین امنیت ملی و بین‌المللی اطلاعات؛

۱۰) تمهید شرایط همکاری میان نهادهای ذیصلاح دولت‌های طرف‌ها حول حوزه‌های کلیدی همکاری احصاء شده در ماده ۳ این موافقت‌نامه و نیز سایرحوزه‌های ممکن در راستای اجرای این موافقت‌نامه؛

۱۱)گسترش همکاری‌ها و هماهنگی فعالیت‌های دولت‌های طرف‌ها در حوزه امنیت بین‌المللی اطلاعات در چارچوب سازمان‌ها و مجامع بین‌المللی (از جمله سازمان ملل متحد، اتحادیه بین‌المللی مخابرات، سازمان بین‌المللی استاندارد، اینترپل، سازمان همکاری شانگ‌های و دیگر سازمان‌های منطقه‌ای و بین‌المللی ذیربط)؛

۱۲) طبق قوانین دولت‌های طرف‌ها، کمک در حوزه‌های انتقال دانش و فناوری اطلاعات؛ ظرفیت‌سازی، توسعه ظرفیت‌ها و آموزش؛ و نیز بررسی امکان سرمایه‌گذاری در زیرساخت‌های امنیت اطلاعات؛

۱۳)کمک به همکاری میان موسسات علمی و آموزشی و نیز بخش‌های خصوصی در حوزه امنیت اطلاعات؛

۱۴) برگزاری نشست‌ها، فراهمایی‌ها (کنفرانس‌ها)، کارگاه‌های آموزشی و دیگر همایش‌های کاری دوجانبه در حوزه‌های تعیین شده همکاری، و نیز برگزاری مشترک و میزبانی رویدادهای منطقه‌ای و بین‌المللی در زمینه امنیت ملی و بین‌المللی اطلاعات.

۲. طرف‌ها یا نهادهای ذیصلاح دولت‌های طرف‌ها می‌توانند براساس توافق متقابل، سایر حوزه‌های همکاری را تعیین نمایند.

دفتر هیئت دولت

ماده ۴

اصول کلی همکاری

۱. طرف‌ها، در چارچوب این موافقت‌نامه، در حوزه امنیت ملی و بین‌المللی اطلاعات به گونه‌ای همکاری خواهند کرد که چنین همکاری موجب ارتقای توسعه اجتماعی و اقتصادی شود، هدف حفظ صلح، امنیت و ثبات بین‌المللی را تامین کند و با قوانین و مقررات داخلی خود و با اصول و هنجارهای پذیرفته شده جهانی حقوق بین‌الملل، شامل اصول احترام متقابل به حاکمیت و تمامیت ارضی، حل و فصل مسالمت‌آمیز اختلافات و مناقشات، عدم بکارگیری زور و تهدید به توسل به زور، عدم دخالت در امور داخلی، احترام به حقوق و آزادی‌های اساسی بشر، و نیز اصول همکاری دوجانبه و عدم دخالت در منابع اطلاعاتِ دولت‌های طرف‌ها منطبق باشد.

۲. فعالیت‌های طرف‌ها در چارچوب این موافقت‌نامه، باید با حق هر طرف، برای جستجو، دریافت و انتشار اطلاعات سازگار باشد؛ با امعان نظر به اینکه چنین حقی می‌تواند به موجب قوانین دولت‌های طرف‌ها به منظورتضمین امنیت ملی محدود شود.

۳. هر یک از طرف‌ها از حقوق برابر برای حفاظت از منابع اطلاعات دولت خود در مقابل استفاده غیرقانونی و دخالت غیرمجاز، از جمله در مقابل حملات رایانه‌ای علیه آنها، برخوردار خواهد بود. هر یک از طرف‌ها متعهد است چنین اقداماتی را علیه طرفِ دیگر بکار نگرفته و به طرف دیگر در استیفای حقوق مذکور کمک کند.

ماده ۵

اشکال و سازوکارهای اصلی همکاری

۱. طرف‌ها نهادهای ذیصلاح دولت‌های خود که مسئولیت اجرای این موافقت‌نامه را برعهده دارند تعیین خواهند کرد و طی ۶۰ روزِکاری از تاریخ لازم‌الاجرا شدن این موافقت‌نامه اطلاعات مربوط به نهادهای ذیصلاح دولت‌های طرف‌ها را مشخص و از طریق مجاری دیپلماتیک تبادل خواهند کرد.

۲. نهادهای ذیصلاح دولت‌های طرف‌ها می‌توانند موافقت‌نامه‌های بین-نهادی ذیربط را با هدف ایجاد چارچوب حقوقی و سازمانی برای همکاری در حوزه‌های خاص همکاری در این موافقت‌نامه منعقد کنند.

۳. به‌منظور بازبینی روند پیشرفت اجرای این موافقت‌نامه، بررسی مسائل پدید آمده در فرایند اجرای آن، تبادل داده‌ها، تحلیل و ارزیابیِ مشترکِ تهدیدهای نوظهور علیه امنیت بین‌المللی اطلاعات، و نیز تعیین، توافق و هماهنگی در خصوص اقدامات واکنشی مشترک در مقابل این تهدیدات، طرف‌ها باید نشست‌های «سازوکارمشورتی منظم»را با شرکت نمایندگان مجاز و نهادهای ذیصلاح خود حداقل یکبار در سال و به نوبت در جمهوری اسلامی ایران و فدراسیون روسیه برگزار نمایند.

ماده ۶

حفاظت از اطلاعات

۱. طرف‌ها، از اطلاعاتی که به موجب این موافقت‌نامه، منتقل شده و یا تولید می‌شوند و دسترسی به آنها طبق قوانین دولت‌های طرف‌ها محدود است، به‌طور مقتضی حفاظت خواهند کرد.

۲.هیچیک از طرف‌ها بدون موافقت کتبیِ قبلیِ طرفِ دیگر، اطلاعات بدست آمده یا مشترکا تولید شده مربوط به اجرای این موافقت‌نامه را برای طرف ثالث فاش نکرده و یا به او انتقال نخواهد داد.

۳. هر یک از طرف‌ها، ضرورتِ محرمانه ماندن اطلاعات مربوط به ابعاد مشخصی از همکاری بین دولت‌های طرف‌ها یا دیگر داده‌ها را به‌موقع به اطلاع طرف دیگر خواهد رساند.

۴. هر اطلاعاتی که درچارچوب این موافقت‌نامه انتقال می‌یابد، صرفا برای اهداف این موافقت‌نامه مورد استفاده قرار خواهد گرفت؛ اطلاعاتی که به‌واسطه فعالیت‌های یکی از طرف‌ها به دست می‌آید، به زیانِ طرف دیگر مورد استفاده قرار نخواهد گرفت.

۵. هر اطلاعاتی که دسترسی به آن محدودیت دارد، طبق قوانینِ دولت‌های طرف‌ها حفاظت خواهد شد.

۶. انتقال و حفاظت از اطلاعاتِ طبقه‌بندی شده، تابع«موافقت‌نامه میان دولت جمهوری اسلامی ایران و دولت فدراسیون روسیه در مورد حفاظت متقابل از اطلاعات طبقه‌بندی شده»۱۷ بهمن ۱۳۸۶(۶ فوریه ۲۰۰۸) خواهد بود.

ماده ۷

تامین مالی

۱. طرف‌ها، هزینه‌های شرکت نمایندگان و کارشناسان خود در رویدادهای مربوط به اجرای این موافقت‌نامه را مستقلا بر عهده خواهند گرفت.

۲. در ارتباط با دیگر هزینه‌های مربوط به اجرای این موافقت‌نامه، طرف‌ها می‌توانند در هر مورد خاص، طبق قوانین دولت‌های خود، روبه‌های مالی دیگری را مورد توافق قرار دهند.

ماده ۸

حل و فصل اختلاف‌ها

طرف‌ها اختلاف‌های ناشی از تفسیر یا اجرای این موافقت‌نامه را از طریق رایزنی و مذاکره میان نهادهای ذیصلاح دولت‌های طرف‌ها و از طریق مجاریِ دیپلماتیک حل و فصل خواهند کرد.

ماده ۹

مفاد پایانی

۱. این موافقت‌نامه در سی امین روز از تاریخ دریافت آخرین اعلانِ کتبی، از طریق مجاری دیپلماتیک، مبنی بر انجام تشریفات داخلی توسط طرف‌ها که برای لازم الاجرا شدن ضروری است لازم‌الاجرا خواهد شد.

۲. طرف‌ها می‌توانند اصلاحاتی را براساس توافق متقابل طرف‌ها و در قالب یک پروتکل مجزا در این موافقت‌نامه اعمال نمایند.

۳. این موافقت‌نامه می‌تواند نود روز پس از دریافت اعلانِ کتبی یکی از طرف‌ها توسط طرف دیگر، از طریق مجاری دیپلماتیک، مبنی بر قصد خود برای فسخ این موافقت‌نامه، فسخ شود.

۴. درصورت فسخ این موافقت‌نامه، طرف‌ها اقداماتی را برای ایفای تعهدات خود مربوط به حفاظت از اطلاعات انجام خواهند داد و اجرای فعالیت‌ها و طرح‌های مشترک و دیگر ابتکاراتی را که پیشتر مورد توافق قرار گرفته‌اند و به موجب این موافقت‌نامه به اجرا در می‌آیند و در زمان فسخ این موافقت‌نامه ناتمام مانده‌اند، تضمین خواهند کرد.

این موافقت‌نامه در مسکو در تاریخ ۷ بهمن ۱۳۹۹ هجری شمسی برابر با ۲۶ ژانویه ۲۰۲۱ میلادی در دو نسخه اصلی به زبان‌های فارسی، روسی و انگلیسی تنظیم شد که تمامی متون از اعتبار یکسانی برخوردار هستند. در صورت بروز اختلاف، نسخه انگلیسی مورد استفاده قرار خواهد گرفت.

ازطرف دولت جمهوری اسلامی ایران **از طرف دولت فدراسیون روسیه**

دفتر هیئت دولت

پیوست

موافقتنامه بین

دولت جمهوری اسلامی ایران و دولت فدراسیون روسیه

در خصوص همکاری در حوزه امنیت اطلاعات

واژگان اصلی

مورد استفاده در موافقت‌نامه بین دولت جمهوری اسلامی ایران و

دولت فدراسیون روسیه در خصوص همکاری در حوزه امنیت اطلاعات

۱. **امنیتِ اطلاعات** به معنای وضعیتی است که در آن افراد، جامعه و دولت و منافع آنها در مقابل تهدیدها،آثار مخرب و سایر آثار منفی در فضای اطلاعات محفوظ هستند.

۲. **امنیتِ بین‌المللی اطلاعات** به معنای وضعیتی در روابط بین‌الملل است که درآن، فضای اطلاعات باعث تضعیف ثبات جهانی و درخطر افتادن امنیت ملت‌ها و جامعه جهانی نگردد.

۳. **فضایِ اطلاعات** به معنای محیطی ناشی از شکل‌گیری، تولید، تبدیل،انتقال، استفاده و ذخیره اطلاعات است و از جمله بر آگاهی‌های فردی و اجتماعی، زیرساختِ اطلاعات و خودِ اطلاعات تاثیر می‌گذارد.

۴. **تهدید علیه امنیتِ اطلاعات** به معنای ترکیبی از اقدامات و عناصری است که خطرِ صدمه به "امنیت اطلاعات" را ایجاد می‌کند.

۵. **زیرساختِ اطلاعات** به معنای طیفی از ابزارها و سامانه‌های (سیستم‌های) فنی برای شکل‌گیری، تولید، تبدیل، انتقال، استفاده و ذخیره اطلاعات می‌باشد.

۶. **زیرساخت‌هایِ حیاتیِ اطلاعات** به معنای سامانه‌های (سیستم‌های) اطلاعات، شبکه‌های اطلاعات و ارتباطات، و دستگاه‌های کنترلِ خودکار می‌باشند که براساس قوانین دولت‌های طرف‌ها تعیین می‌شوند.

۷. **حادثه رایانه‌ای** به معنای وقوع اخلال و (یا)غیرفعال شدن تاسیسات زیرساختِ اطلاعات، یک شبکه ارتباطات الکترونیکی که برای سازماندهی تعامل بین چنین تاسیساتی استفاده می‌شود و (یا) نقضِ امنیتِ اطلاعاتِ پردازش شده توسط چنین تاسیساتی می‌باشد که دراثر یک حمله رایانه‌ای هم اتفاق می‌افتند،

۸. **حمله رایانه‌ای** به معنای تاثیر هدفمند توسط نرم افزار و (یا) سخت افزار بر تاسیسات زیرساخت‌های اطلاعات، و بر یک شبکه ارتباطات الکترونیکی که برای سازماندهی تعامل بین چنین تاسیساتی، با هدف وقفه و (یا) غیرفعال‌سازی آنها و (یا) به خطر انداختن امنیت اطلاعاتِ پردازش شده توسطِ چنین تاسیسات اطلاعات استفاده می‌شود.

AGREEMENT
between The Government of the Islamic Republic of Iran and The Government of the Russian Federation on Cooperation in the Field of Information Security

The Government of the Islamic Republic of Iran and the Government of the Russian Federation, hereinafter referred to as the Parties,

Referring to the Treaty on the Basis for Mutual Relations and Principles of Cooperation between the Islamic Republic of Iran and the Russian Federation of 22 Bahman 1379 (March 12, 2001),

Noting that considerable progress has been achieved in the development and implementation of the latest information and communication technologies,

Noting great importance of information and communication technologies in social and economic development for the benefit of the humanity and in maintaining international peace, security and stability in the contemporary world,

Expressing concern over the threats posed by the possible use of such technologies for the purposes inconsistent with aims of ensuring international peace, security and stability, for undermining sovereignty and security of States and interfering in their internal affairs, violating citizens' privacy, destabilizing domestic political, social and economic situation, fomenting interethnic and interreligious hostility,

Emphasizing the need to maximize their common benefits from information and communication technologies and to reduce common threats against them therefrom,

Emphasizing also on the imperative of respecting laws and regulations of the States of the Parties in the implementation of this Agreement,

AGREEMENT
between The Government of the Islamic Republic of Iran and The Government of the Russian Federation on Cooperation in the Field of Information Security

The Government of the Islamic Republic of Iran and the Government of the Russian Federation, hereinafter referred to as the Parties,

Referring to the Treaty on the Basic for Mutual Relations and Principles of Cooperation between the Islamic Republic of Iran and the Russian Federation of 22 Esfand 1379 (March 12, 2001),

Noting that considerable progress has been achieved in the development and implementation of the latest information and communication technologies,

Noting great importance of informatied and communication technologies in social and economic development for the benefit of the humanity and in maintaining international peace, security and stability in the contemporary world,

Expressing concern over the threats posed by the possible use of such technologies for the purposes inconsistent with aims of ensuring international peace, security and stability, for undermining sovereignty and security of States and interfering in their internal affairs, violating citizens' privacy, destabilizing domestic political, social and economic situation, fomenting interethnic and interreligious hostility,

Emphasizing the need to maximize their common benefits from information and communication technologies and to reduce common threats against them therefrom,

Emphasizing also on the imperative of respecting laws and regulations of the States of the Parties in the implementation of this Agreement,

Emphasizing also the importance of respecting laws and regulations of the States of the Parties in the implementation of this Agreement,

Acknowledging increasing importance of information security in international security system,

Affirming that State sovereignty and international norms and principles resulting from State sovereignty apply to State conduct within the framework of information and communication technologies related activities, and to their jurisdiction over information and communication technologies infrastructure within their territory, and affirming also that States have sovereign right to define and implement State policy on matters relating to information and telecommunication Internet networks, including ensuring security,

Convinced that further build-up of trust and development of cooperation in the area of information and communication technologies between the Parties are an urgent necessity and serve their interests,

Attaching great importance to the balance between ensuring security and respecting human rights in the area of the use of information and communication technologies, in accordance with the national legislation, as well as international obligations of the States of the Parties,

Seeking to prevent and counter threats to information security, to ensure information security interests of the States of the Parties in order to create a peaceful and secure international information environment,

Condemning unilateral coercive measures taken in violation of the UN Charter,

Seeking further joint work to mitigate the vulnerabilities of States' critical infrastructure to information security, including the threats of potential hacking and blocking measures in ICTs and Internet access against the States of the Parties,

Seeking also to closely cooperate in regional and international fora, to develop and promote legal means and rules to ensure international information security, including through their increased governance,

Wishing to establish a mutual framework for the cooperation between the States of the Parties in the field of information security,

Have agreed as follows:

Article 1

Basic Terms

1. For the purposes of implementation of this Agreement, the Parties agree on the definitions of the basic terms as specified in the Annex, which is an integral part of this Agreement.

2. The Annex may, if necessary, be supplemented, amended and updated as agreed by the Parties.

Article 2

Main Threats in the Field of Information Security

While cooperating under this Agreement, the Parties shall proceed from the fact that the main threats to information security are posed by the use of information and communication technologies, including:

(1) for change and aimed at violating sovereignty, security and territorial integrity of States;

(2) to cause economic and other damage, including by making destructive impact upon critical information and other relevant information infrastructure facilities;

(3) for terrorist purposes, including terrorist propaganda and recruitment for terrorist activities;

(4) to commit crimes, including those related to unauthorized access to computer information;

(5) to interfere into internal affairs of States, violate public order, incite interethnic, interracial and inter-religious hostility, disseminate racist and xenophobic ideas and theories which ignite hatred and discrimination and incite violence and instability, and to destabilize domestic political, social and economic situation and interfere with State governance;

(6) to disseminate information harmful for socio-political and socio-economic systems, as well as for spiritual, moral and cultural environment of other States.

Article 3

Main Areas of Bilateral Cooperation

1. Taking due account the main threats listed in article 2 of this Agreement, and the need to ensure information security, the Parties, their authorized representatives and competent authorities of the States of the Parties defined in accordance with article 5 of this Agreement shall cooperate on such issues as enhancing information security, combating crimes committed with the use of information and communication technologies, technical and technological assistance, and international cooperation among others, in the following key areas:

(1) identifying, coordinating and implementing necessary cooperation in the regional and international forums to ensure national and international information security;

(2) elaborating and promoting norms of applicable international law to ensure national and international information security;

(3) countering the threats in the field of ensuring information security as defined in article 2 of this Agreement;

(4) exchanging information and cooperating in the field of law enforcement in order to prevent, detect, combat, investigate and prosecute crimes involving the use of information and communication technologies for terrorist and criminal purposes;

(5) contributing to multilateral negotiations on confidence building measures relating to international information security;

(6) exchanging information between competent authorities of the States of the Parties in the field of information security, including cooperation between relevant authorities of the States of the Parties in the area of computer incident response;

(7) exchanging information on the national legislation of the States of the Parties related to ensuring information security;

(8) cooperating to address negative impacts in the area of ensuring information security caused by unilateral coercive measures taken in violation of the UN Charter and international law;

(9) promoting the improvement of the bilateral legal framework and practical mechanisms for cooperation between the States of the Parties in ensuring national and international information security;

(10) creating conditions for cooperation between competent authorities of the States of the Parties on key areas of cooperation.

outlined in article 3 of this Agreement, as well as on other possible areas in order to implement this Agreement;

(11) Intensifying cooperation and coordination of activity of the bodies of the Parties in the area of international information security within the framework of international organizations and fora (including the United Nations, International Telecommunications Union, International Standardization Organization, Interpol, Shanghai Cooperation Organization and other relevant regional and international organizations);

(12) Assisting according to the legislation of the States of the Parties in areas of transfer of information technology and knowledge, capacity building and development and training, as well as exploring possible investment in the information security infrastructures;

(13) assisting in cooperation among scientific and educational institutions as well as private sectors in the field of information security;

(14) Holding bilateral working meetings, conferences, workshops and other forums in the specified areas of cooperation, as well as co-sponsoring and hosting of regional and international events in field of national and international information security.

2. The Parties or competent authorities of the States of the Parties may, by mutual agreement, determine other areas of cooperation.

Article 4

General Principles of Cooperation

1. The Parties shall cooperate in the field of national and international information security within the framework of this Agreement in such a way that such cooperation would promote social

and economic development and would meet the objective of maintaining international peace, security and stability and comply with their national laws and regulations and the universally accepted principles and norms of international law, including the principles of mutual respect for sovereignty and territorial integrity, peaceful settlement of disputes and conflicts, non-use of force or threat of force, non-interference in internal affairs, respect for fundamental human rights and freedoms, as well as the principles of bilateral cooperation and non-interference in information resources of the States of the Parties.

2. The activities of the Parties within the framework of this Agreement shall be comparable with the right of each Party to seek, receive and disseminate information taking into account the fact that this right can be limited by the legislation of the States of the Parties in order to ensure national security.

3. Each of the Parties shall have equal rights to protect information resources of its State from unlawful use and unauthorized interference, including computer attacks against them. Each of the Parties undertakes not to take such actions against the other Party and shall assist the other Party in fulfilling the rights mentioned above.

Article 5
Main Forms and Mechanisms of Cooperation

1. The Parties shall identify competent authorities of the States of the Parties responsible for the implementation of this Agreement and, within 60 days after the date of entry into force of this Agreement, shall designate and exchange through diplomatic channels information about the competent authorities of the States of the Parties.

2. In order to establish legal and organizational framework for cooperation in specific areas of cooperation under this Agreement, the competent authorities of the States of the Parties may conclude relevant inter-agency agreements.

3. In order to review the progress of the implementation of this Agreement, to consider issues arising in the course of its implementation, to exchange data, analyze and jointly assess emerging threats to international information security, as well as to determine, agree upon and coordinate joint response measures to such threats, the Parties shall organize Regular Consultation Mechanism, attended by their authorized representatives and competent authorities, on the ground, both, at least once a year, in the Islamic Republic of Iran and the Russian Federation.

Article 6

Protection of Information

1. The Parties shall provide appropriate protection of the information which is transferred or generated under this Agreement and access to which is limited by the legislation of the States of the Parties.

2. Each Party shall not disclose or transfer to a third party information obtained or jointly generated/related to the implementation of this Agreement without prior written consent of the other Party.

3. Each Party shall timely notify the other Party of the need to keep confidential the information regarding certain aspects of cooperation between the States of the Parties or other data.

4. Any information transferred under this Agreement shall be used only for the purposes of this Agreement. Information obtained

for one of the Parties activities shall not be used to detriment of the other Party.

3. Any restricted-access information shall be protected in accordance with the legislation of the States of the Parties.

4. Transfer and protection of classified information shall be regulated by the Agreement between the Government of the Islamic Republic of Iran and the Government of the Russian Federation on Mutual Protection of Classified Information of 17 February 1998 (Tehran, 2003).

Article 7
Financing

1. The Parties shall independently bear the costs of the implementation of their representatives and experts in respective events related to implementation of this Agreement.

2. Concerning other costs related to the implementation of this Agreement, the Parties may agree upon other financial procedures in each particular case in accordance with the legislation of their States.

Article 8
Settlement of Disputes

The Parties shall settle the disputes that may arise out of the interpretation or implementation of this Agreement, through consultations and negotiations between competent authorities of the States of the Parties and, through diplomatic channels.

Article 9
Final Provisions

1. This Agreement shall enter into force on the 30th day following the date of receipt, through diplomatic channels, of the last written notification on the completion by the Parties of internal procedures necessary for its entry into force.

2. The Parties may make amendments to this Agreement, which shall be, by mutual consent of the Parties, formalized as a separate protocol.

3. This Agreement may be terminated 90 days after the receipt by either of the Parties, through diplomatic channels, of a written notification from the other Party, of its intention to terminate this Agreement.

4. In case of termination of this Agreement, the Parties shall take measures to fulfill their obligations related to information protection and shall ensure the implementation of the formerly agreed joint activities, projects and other initiatives carried out under this Agreement and not completed at the time of termination of this Agreement.

Done in Moscow, 7 Bahman 1399 (January 26, 2021), in two original copies, each in the Persian, Russian, and English languages, all texts being equally authentic. In case of divergence, the English version shall be used.

For the Government of the Islamic Republic of Iran

For the Government of the Russian Federation

ANNEX to the Agreement between the Government of the Islamic Republic of Iran and the Government of the Russian Federation on Cooperation in the Field of Information Security

BASIC TERMS

used in the Agreement between the Government of the Islamic Republic of Iran and the Government of the Russian Federation on Cooperation in the Field of Information Security

1. *Information security* means the State of individuals, society and the State and their interests when they are protected from threats, destructive and other negative impacts in the information space.

2. *International information security* means the state of international relations that excludes undermining global stability and endangering the security of nations and the world community in the information space.

3. *Information space* means the environment resulting from the formation, generation, transformation, transmission, use, storage of information that have an impact, among others, on individual and social consciousness, information infrastructure and information itself.

4. *Threats to information security* means a combination of actions and factors creating risk of damaging the "information security".

5. *Information infrastructure* means a range of technical tools and systems for formation, generation, transformation, transmission, use and storage of information.

دفتر هیئت دولت

6. *Critical information infrastructures* means information systems, information and telecommunications networks, automated control systems defined in accordance with the legislation of the States of the Parties;

7. *Computer incident* means a fact of disruption and (or) inactivation of an information infrastructure facility, an electronic communications network, used to organize the interaction of such facilities, and (or) breaches of security of information processed by such facility, which also took place as a result of a computer attack;

8. *Computer attack* means purposeful influence by software and (or) [illegible] information infrastructure facilities, an electronic communications network, used to organize the interaction of such facilities, and (or) [illegible] to endanger the security of information processed by such information facilities.