شماره۱۶۰۱۱/۱/۲۳۰۵ ۱۴۰۱/۸/۱

جناب آقای دکتر اکبرپور

مدیرعامل روزنامه رسمی جمهوری اسلامی ایران

به پیوست یک نسخه از مصوبه شماره ۱۶۰/۱/۲۳۰۱ مورخ ۱۴۰۱/۷/۲۰ با عنوان طرح راهبردی حفاظت از زیرساخت های کشور که در شصت و هفتمین جلسه کمیته ی دائمی (شورای عالی) پدافند غیرعامل کشور به تصویب رسیده است جهت انتشار در روزنامه رسمی به حضورتان ارسال می گردد.

دبیرکمیته دائمی و رئیس سازمان پدافند غیرعامل کشور

سرتیپ پاسدار دکتر غلامرضا جلالی

مقام معظّم رهبری و فرماندهی کل قوا (مدظلّه العالی) ـ ۱۳۹۷/۰۸/۰۶

«هر ملتی هم که به فکر دفاع از خود نباشد و خود را آماده نکند در واقع زنده نیست، هر ملتی هم که اهمیت دفاع را درک نکند به یک معنا زنده نیست ، ما نمی توانیم چشم و قدرت تحلیل داشته باشیم توطئه عمیق عناد آمیز استکبار علیه اسلام و انقلاب و نظام اسلامی را ببینیم در عین حال به فکر دفاع نباشیم خدا آن روز را نیاورد که این ملت و برگزیدگانش از تهاجم عنودانه خباثت آمیز استکبار جهانی و در رأس آنها آمریکا دچار غفلت بشود .»

تصویب نامه

وزیر محترم کشور ـ وزیر محترم دفاع و پشتیبانی نیروهای مسلّح

معاون محترم رئیس جمهور و رئیس سازمان برنامه و بودجه کشور

رئیس محترم کمیسیون امنیت ملّی و سیاست خارجی مجلس شورای اسلامی

سردارمعاون محترم هماهنگ کننده ستادکل نیروهای مسلّح

سردار رئیس محترم سازمان پدافند غیرعامل کشور

به استناد ماده۸ اساسنامه سازمان پدافند غیرعامل کشور مصوّب مقام معظّم رهبری و فرماندهی کلّ قوا (مدظله العالی) در تاریخ ۱۴۰۱/۰۶/۲۹ شصت وششمین جلسه کمیته دائمی (شورای عالی) پدافند غیرعامل کشور تشکیل و طرح راهبـردی حفاظت از زیرسـاخت های کشـور موضـوع مادّه نه اساسنامه، پیشنهادی آن سازمـان را بررسی و به شرح زیر تصویب نمود؛

طـرح راهبـردی حفـاظت از زیـرساخت های کشـور

مقدمه

زیرساخت های هر کشور، بستر مهم حیات، رشد و پویایی آن به شمار می رود، برخی از زیرساخت ها نقشی حیاتی در حفظ منافع ملی دارند و بعنوان یکی از ارکان مهم پیشرفت، اختلال هرچند کوتاه مدت در عملکرد آنها می تواند منجر به آسیب جدی در اقتصاد و امنیت ملی شود؛ از آنجا که زیرساخت ها، جریانی به هم پیوسته از خدمات و پشتیبانی ها را برای تأمین نیازهای اساسی به جامعه ارائه می دهند و آسیب یا اختلال در عملکرد و کارکرد آنها می تواند قطع خدمات زیرساختی به مردم و جامعه را در پی داشته باشد؛ از این رو طرح راهبردی حفاظت از زیرساخت های کشور، به عنوان عالی ترین سند پدافند کالبدی و حفاظت از زیرساخت های کشور، در راستای مصون سازی زیرساخت ها و شریان های حیاتی و حفظ و تضمین تداوم ارائه خدمات ضروری به بخش های مختلف جامعه و مردم تدوین شده است.

ماده۱ـ تعاریف و اختصارات

۱) سازمان: سازمان پدافند غیرعامل کشور

۲) کمیته دائمی: کمیته دائمی پدافند غیرعامل کشور

۳) زیرساخت۱: به مجموعه ای از مراکز و تأسیسات زیربنایی و شریان های عمده که خدمات و نیازهای ضروری و اساسی کشور را به مردم و جامعه ارائه می کند، اطلاق می گردد؛ زیرساخت مشتمل بر فرابخش۲(حوزه)، بخش۳، زیربخش۴، دارایی۵ و اجزاء آن می باشد.

۴) حوزه های با اهمیت بالا۶: به هریک از حوزه های ۱ـ انرژی، ۲ـ آب، ۳ـ غذا و کشاورزی، ۴ـ حمل و نقل، ۵ ـ بهداشت و سلامت، ۶ ـ دفاعی و امنیتی، ۷ـ صنعت، ۸ ـ رسانه، ۹ـ هسته ای، ۱۰ـ فضا، ۱۱ـ جمعیت، ۱۲ـ حاکمیتی، ۱۳ـ خدمات ضروری و فوریتی، ۱۴ـ پولی و مالی، ۱۵ ـ ارتباطات و فناوری اطلاعات، حوزه های با اهمیت بالا گفته می شود که باتوجه به شاخص های زیر، حوزه های ؛ ۱ـ انرژی، ۲ـ آب، ۳ـ ارتباطات و فناوری اطلاعات، ۴ـ حمل و نقل، ۵ ـ بهداشت و سلامت، ۶ ـ غذا و کشاورزی، ۷ـ دفاعی و امنیتی و ۸ ـ حاکمیتی بعنوان حوزه های کلیدی از منظر پدافند غیرعامل دسته بندی می شوند :

— اهمیت کارکرد هر حوزه در تأمین نیازهای حیاتی مردم در شرایط اضطراری

— شدت اثرگذاری بر اقتصاد، امنیت ملی و سلامت مردم

— وابستگی زیرساخت های سایر حوزه ها به عملکرد آنها

— شدّت پیامد وقوع تهدید مبتنی بر جغرافیا و جمعیت

۵) پدافند کالبدی: مجموعه تدابیر و اقدامات فنی و مهندسی پدافند غیرعامل که بکارگیری آنها در سطوح راهبردی، عملیاتی و اجرایی در زیرساخت ها موجب تولید بازدارندگی، کاهش آسیب پذیری، تسهیل مدیریت بحران، ارتقاء تاب آوری زیرساختی، آمادگی پاسخ پدافندی به تهدید، پایداری و مصونیت بخشی، مدیریت مخاطرات و تضمین تداوم کارکرد و استمرار خدمات اساسی در برابر تهدیدات و اقدامات نظامی دشمن می شود.

۶) طرح راهبردی: مجموعه ای یکپارچه متشکل از مطلوبیت های راهبردی از قبیل اصول، ارزش ، ماموریت، اهداف کلان و چشم انداز، راهبردها، اقدامات اساسی، برنامه ها، راهبردهای عملیاتی و الزامات تحقق آنهاست که پیاده سازی آن می تواند دستیابی به اهداف را تسهیل کند.

۷) حفاظت از زیرساخت۷: مجموعه تدابیر و اقدامات پدافند غیرعاملی که توانایی و آمادگی عملیاتی زیرساخت و تداوم کارکردهای آن و دستگاه های اجرایی مسئول برای پاسخ مؤثر به حوادث و سوانح ناشی از تهدیدات نظامی، تهدیدات امنیتی و تروریستی، تهدیدات سایبری زیرساختی و تهدیدات از درون دشمن پایه را افزایش می دهد بطوری که فعالیت آن حفظ گردیده و خسارات انسانی و مادی ناشی از آن را به حداقل می رساند.

۸) مخاطره امنیتی ـ نظامی: به اندرکنش تهدیدات با آسیب پذیری ها و احتمال وقوع و شدت پیامد آنها با منشاء دشمن در حوزه های زیستی، سایبری، شیمیایی، پرتوی، تروریستی، امنیتی، نظامی و یا ترکیبی از آنها که با هدف ضربه زدن به امنیت ملی کشور باشد، اطلاق می گردد.

۹) تهدیدات درون زا۸: به تهدیداتی اطلاق می گردد که توسط کارکنان یک سازمان یا شبکه های همکار(پیمانکاران و سایرین) به صورت فردی یا شبکه ای، خواسته یا ناخواسته با همکاری یا هدایت عوامل بیگانه یا بدون پشتیبانی آنها از سطح دسترسی مجاز، دانش و اختیارات خود برای آسیب رساندن به سازمان استفاده کنند این امر می تواند شامل سرقت اطلاعات و فنآوری، خسارت به تأسیسات، سیستم ها، تجهیزات، کارکردها و فرآیندها، صدمه به کارمندان، توقّف فعالیت های ضروری و یا اقدامات دیگری در جهت صدمه زدن به مأموریت سازمان و منافع آن باشد.

۱- Infrastructure

۲- Sector

۳- system

۴- subsystem

۵- Asset & components

۶- Critical infrastructure

۷- infrastructure protection

۸- Insider threat

۱۰) مراکز ضروری: مراکز و تأسیساتی که فقدان یا اختلال در عملکرد آنها زندگی مردم را با چالش مواجه می سازد.

۱۱) شریان های اصلی و حیاتی: به شبکه های زیرساختی و ارتباطی که نقش اصلی و حیاتی در تأمین نیازهای اساسی اداره کشور و امور مردم را دارند اطلاق می شود؛ مانند شبکه های ارتباطات، آب و گاز و سایر.

۱۲) وابستگی متقابل: عبارت است از ارتباط عملکردی اجزا و فرآیندها به یکدیگر که درصورت اختلال در یک سیستم احتمال ایجاد اختلال در مراکز و تاسیسات وابسته وجود دارد و به انواع فیزیکی، جغرافیایی، سایبری و منطقی تقسیم می شود.

۱۳) سطح بندی: میزان ارزش و اهمیت مراکز، تاسیسات و زیرساخت های کشور است که از منظر پدافند غیرعامل در سطوح حیاتی، حساس، مهم و قابل حفاظت تقسیم بندی و تعریف می شوند.

۱۴) روابط سیستمی زیرساختی: روابط حاکم بر زیرساخت ها مبتنی بر رویکرد سیستم از سیستم۱ و تعامل بین اجزای سیستم زیرساختی که منجر به ایجاد روابط سیستمی از قبیل هم افزایی، تضاد، وابستگی و وابستگی متقابل می شود.

۱۵) آسیب پذیری۲: میزان خسارات و صدماتی است که از عوامل و پدیده های بالقوه (تهدیدات) یا بالفعل خسارت زا به نیروی انسانی، تجهیزات و تأسیسات با شدت صفر تا صد درصد ناشی می گردد.

۱۶) تاب آوری۳: به توانایی یک نظام، جامعه، دستگاه اجرایی و یا زیرساخت برای ایستادگی، تحمّل، انعطاف پذیری و حفظ کارکرد، تطبیق و برگشت پذیری در برابر مخاطره امنیتی ـ نظامی گفته می شود.

۱۷) تداوم کارکرد۴: توانایی ادامه تولید محصولات یا ارائه خدمات توسط زیرساخت ها در چارچوب زمانی مورد پذیرش، قابل قبول و درحد ظرفیت از پیش تعیین شده، حین و پس از وقوع مخاطره امنیتی ـ نظامی، تداوم کارکرد گفته می شود.

ماده۲ـ اسناد بالادستی

۱) فرامین، تدابیر و منویات مقام معظم رهبری(مدظله العالی)

۲) سیاست های کلی نظام در موضوع پدافند غیرعامل و آمایش سرزمین

۳) قانون احکام دائمی برنامه های توسعه کشور ـ ماده ۵۸

۴) سند جهت گیری های ملّی آمایش سرزمین ـ بندهای ۸۰ ، ۸۱ و ۸۲ از ماده۱

۵) اساسنامه سازمان پدافند غیرعامل کشور

۶) قانون برنامه پنج ساله ششم توسعه جمهوری اسلامی ایران ـ بند پ ماده۱۰۶

۷) سیاست های کلی برنامه پنج ساله هفتم توسعه جمهوری اسلامی ایران ـ بند ۲۴

ماده۳ـ منظور

۱) ایجاد درک مشترک از مفهوم حفاظت از زیرساخت، تعیین راهبردها، سیاست ها و وظایف اصلی دستگاه های اجرایی متولی حوزه های کلیدی برای دستیابی به اهداف پدافند کالبدی در کشور،

۲) تبیین چارچوبی مدوّن برای تهیه و تنظیم ضوابط و مقررات حفاظت از زیرساخت، برنامه های مصون سازی و ارتقاء آمادگی زیرساخت های حوزه های با اهمیت بالا و شریان های اصلی و حیاتی کشور،

۳) ایجاد هماهنگی، هم سویی و هم افزایی بین سازمان و دستگاه های اجرایی متولی حوزه های بااهمیت بالای کشور در راستای حفظ و ارتقاء پایداری ملی در شرایط اضطراری ناشی از وقوع تهدید،

ماده۴ـ حوزه شمول و حدود کاربرد طرح

الف) دستگاه های اجرایی متولی زیرساخت های حیاتی، حساس، مهم و قابل حفاظت (زیرساخت های در دست مطالعه، اجرا، ساخت و درحال بهره برداری) در هر یک از حوزه های با اهمیت بالای کشور

ب) سازمان های نیروهای مسلح دارای زیرساخت های صنعتی ـ اقتصادی مانند؛ نیروگاه، پالایشگاه و سایر

ج) بخش خصوصی و غیردولتی دارای زیرساخت های حیاتی، حساس، مهم و قابل حفاظت در حوزه های با اهمیت بالا

۱- System of system

۲- Vulnerability

۳- Resiliency

۴- Business continuity

د) حدود کاربرد طرح در سلسله مراتب طرح های پدافند کالبدی زیر است :

۱) طرح های پدافند کالبدی زیرساخت دستگاهی: مطالعات پدافند غیرعامل زیرساخت های حوزه شمول (ماده۴ این طرح)

۲) طرح های پدافند غیرعامل شهری: مطالعات پدافند غیرعامل زیرساخت های شهری

۳) طرح های جامع پدافند غیرعامل استانی: طرح ها و برنامه های پدافند غیرعامل استان و شهرستان

۴) طرح های جامع موضوعی پدافند کالبدی و حفاظت از زیرساخت کشور: طرح های راهبردی و ملی در موضوعات اساسی زیرساختی کشور مانند طرح جامع پدافند غیرعامل حفاظت از زیرساخت ـ SSP۱ ـ آب، برق، گاز و پتروشیمی

۵) طرح راهبردی و ملی حفاظت از زیرساخت ها و شریان های حائز اهمیت کشور

ماده۵ ـ اصول و ارزش ها

۱) اقتدار ذاتی و درون زای زیرساختی

۲) خوداتکائی ملی (عدم پذیرش تسلط کفار بر مسلمانان)

۳) صیانت از منافع ملی

۴) قوی شدن مبتنی بر دانش، فناوری و صنعت

۵) قابلیت دفاع ذاتی

۶) پایداری در برابر تهدیدات

۷) تاب آوری زیرساختی

۸) تداوم کارکرد زیرساختی و خدمات ضروری

۹) تناسب اهمیت با امنیت زیرساخت

۱۰) کاهش مستمر آسیب پذیری

۱۱) حفاظت همه جانبه در برابر تهدیدات

۱۲) آمادگی دائمی پاسخ به تهدید

۱۳) مدیریت ریسک و مخاطرات

۱۴) روزآمدی اقدامات پدافندی

۱۵) مهندسی ارزش (هزینه ـ فایده)

۱۶) تقدّم امنیت بر توسعه

۱۷) پدافند عمیق و لایه به لایه

۱۸) توسعه ی امنیت افزا و ذاتاً اَمن

۱۹) حفظ سرمایه های ملی

ماده۶ ـ تهدیدات مفروض

تهدیدات مفروض این طرح عبارتند از:

۱) تهدیدات نظامی (هوایی، زمینی، دریایی، موشکی)

۲) تهدیدات امنیتی و تروریستی (اقدامات ضد زیرساختی تروریستی)

۳) تهدیدات سایبری زیرساختی (تهدیدات زیرساختی سایبری علیه زیرساخت های هوشمند)

۴) تهدیدات از درونِ دشمن پایه

تبصره: این طرح سایر تهدیدات نوین و نوپدید با منشاء دشمن و ترکیبی از آنها که با هدف تخریب و اختلال در عملکرد زیرساخت در آینده با آن مواجه خواهیم شد را نیز شامل می شود.

ماده۷ـ اهداف و مأموریت های عمده

اهداف و مأموریت های عمده در طرح راهبردی حفاظت از زیرساخت های کشور عبارت است از:

۱) سطح بندی روزآمد زیرساخت ها و دارایی های حوزه های با اهمیت بالا،

۲) رصد و پایش، تشخیص، هشدار و مدیریت تهدیدات زیرساختی ،

۳) مصون سازی، امن سازی، تاب آور نمودن زیرساخت ها متناسب با سطح اهمیت انها،

۴) تضمین و تسهیل تداوم کارکرد و استمرار خدمات ضروری زیرساخت های حیاتی در کشور،

۵) بهینه سازی سطح وابستگی و کاهش مستمر آسیب پذیری در زیرساخت ها متناسب با سطح اهمیت آن ها،

۶) نهادینه سازی اصول و الزامات پدافند غیرعامل در ذات طرح های توسعه زیرساختی کشور،

۱- Sector Specific Plan

۷) کاهش و خنثی سازی درونی و ذاتی مخاطرات زیرساخت های دارای پتانسیل خطر در زمان طراحی و ساخت،

۸) مصونیت زیرساخت های سایبری و وابسته به سایبر و هوشمند،

۹) پاسخ به حوادث و تهدیدات و ایجاد آمادگی در برابر آنها در زیرساخت های حوزه های با اهمیت بالا،

۱۰) مدیریت و کاهش تهدیدات درون زا در زیرساخت های حوزه های با اهمیت بالا،

۱۱) توانمندسازی و آموزش مدیران و کارکنان دستگاه های متولی راهبری زیرساخت های حوزه های با اهمیت بالا،

۱۲) هماهنگی حداکثری و هم افزایی دستگاهی برای ارتقاء آمادگی های عملیاتی و تداوم کارکردهای ضروری،

ماده۸ ـ راهبردها

۱) سطح بندی زیرساخت ها مبتنی بر مؤلفه های ماهیت، اهمیت، هوشمندی، کارکرد، سیستمی یا غیرسیستمی بودن و خطرزایی با نظام روزآمد سطح بندی زیرساخت ها و دارایی ها،

۲) نهادینه سازی اصول، الزامات و ملاحظات حفاظت از زیرساخت در ذات طرح های توسعه زیرساخت در برابر انواع تهدیدات (مهاجرت پدافند از پیوست به ذات طرح) از طریق:

۱ـ مصون سازی در لایه طرح های پایه با چارچوب های فنی و مهندسی با رعایت اندرکنش سیستمی زیرساخت ها

۲ـ مصون سازی با تأکید بر انتخاب فناوری مورد نیاز طرح و پیش بینی الزامات پدافندی در ذات فناوری و طرح

۳) توسعه و پیاده سازی سامانه رصد، پایش، ارزیابی، تشخیص و هشداردهی روزآمد تهدیدات و آسیب پذیری ها در زیرساخت ها و شریان های حیاتی و شبکه سازی آن در قالب سامانه یکپارچه ملی،

۴) ارتقاء امنیت و پایداری زیرساخت ها و شریان های حیاتی کشور با تهیه طرح های جامع عملیاتی پدافندی در جهت مصون سازی، افزایش آمادگی، ارتقاء تاب آوری و اَمن سازی اضطراری ـ EOP۱ ـ با رویکرد زیست بوم، متمرکز بر اقدامات اساسی زیر:

۱ـ تهیه و پیاده سازی طرح پاسخ اضطراری به حوادث و تهدیدات زیرساختی ـ ERP۲

۲ـ تهیه و پیاده سازی طرح تضمین و تسهیل تداوم کارکردهای اساسی ـ BCP۳

۳ـ تهیه و پیاده سازی طرح بازیابی و برگشت پذیری زیرساختی و سیستمی ـ DRP۴

۴ـ تهیه و پیاده سازی طرح اَمن سازی و مصون سازی و تاب آوری ـ ISP۵

۵ ـ تهیه و پیاده سازی طرح کاهش آسیب پذیری ـ VRP۶

۶ ـ تهیه و پیاده سازی طرح بهینه سازی وابستگی و وابستگی های متقابل ـ OIP۷

۷ـ تهیه و پیاده سازی طرح های ارزیابی و ارتقاء آمادگی های زیرساختی ـ PPP۸

۵) حفظ و تداوم کارکردهای ضروری و تأمین نیازهای اساسی کشور از طریق طراحی، پیاده سازی و روزآمدسازی نظام عملیاتی حفظ و تداوم کارکرد زیرساخت ها،

۶) پایدارسازی و تاب آور نمودن زیرساخت های حیاتی با قابلیت برگشت پذیری سریع ، انعطاف پذیر بودن در برابر تهدیدات، مقاوم بودن در برابر حوادث، حفظ تداوم عملکرد، ارتقاء ضریب افزونگی با تمرکز بر حفظ کارکرد اصلی در سطح پاسخگویی به نیاز،

۷) بهینه سازی وابستگی متقابل در زیرساخت های حیاتی کشور از طریق ذخیره سازی، اَمن سازی، جایگزینی خدمات، تطبیق پذیری با تمرکز بر برطرف نمودن یا موازی نمودن گره های زنجیره تولیدات و خدمات،

۸) استفاده حداکثری از ظرفیت های دستگاهی با تاکید بر تداوم کارکرد زنجیره فعالیت /خدمت از طریق نقش پذیری مناسب دستگاه های ذی نقش با هماهنگی و هم افزایی دستگاهی و مدیریت و فرماندهی یکپارچه،

۹) طراحی، پیاده سازی نظام، ساختار و الزامات تحقق برنامه کاهش مستمر تهدیدات درون زا با رصد و مراقبت نوبه ای،

۱۰) مصون سازی سایبری همه جانبه، چندلایه و تطبیق پذیر زیرساخت های حائز اهمیت سایبری و وابسته به سایبر کشور در مقابل تهدیدات سایبری دشمن از طریق:

۱ـ شناسایی و ارزیابی دارایی های سایبری و تعیین سطح اهمیت آنها،

۲ـ رصد، پایش، برآورد تهدیدات و اشتراک گذاری اطلاعات،

Emergency operations Plan -۱

Emergency Response Plan -۲

Business Countinuty Plan -۳

Disaster Recovery Plan -۴

Immunius & Security Plan -۵

Vulnerability Reduction Plan -۶

Optimizing Interdependency Plan-۷

Preparedness Promotly Plan -۸

۳ـ رفع یا کاهش آسیب پذیری های سایبری دارایی های سایبری و وابسته به سایبر،

۴ـ برآورد، تحلیل و مدیریت مخاطرات سایبری زیرساخت و پیامدهای آبشاری آن،

۵ ـ نظام مند کردن ساختار امنیت و پدافند سایبری و فرآیندها و نیروی انسانی،

۶ ـ روزآمدسازی و بومی سازی هوشمندی در زیرساخت های حیاتی کشور وابسته به فضای سایبر،

۷ـ حفاظت سایبری از زیرساخت های وابسته به فضای سایبر با تهیه و پیاده سازی طرح های عملیاتی پدافند سایبری ـ CERP۱,CVRP۲,CBCP۳,CDRP۴,CCIP۵,CPPP۶

۱۱) ارتقاء آمادگی حداکثری و توانمندسازی مدیران و کارشناسان دستگاه های متولی راهبری حوزه های با اهمیت بالا با تاکید برتجهیز، تمرین، رزمایش، ارتقاء آمادگی و بازخورد و اصلاح طرح های عملیاتی پدافندی و رزمایش های تخصصی،

۱۲) کاهش و مدیریت مخاطرات زیرساخت های با قابلیت تولید خطر بالا (پرخطر) از طریق:

۱ـ سطح بندی زیرساخت ها از منظر خطرپذیری،

۲ـ آمادگی و پاسخ دائمی به حوادث و رخدادها و مخاطرات،

۳ ـ بهره گیری از رویکرد طراحی و مصون سازی تخصصی در ذات طرح مبتنی بر طراحی ذاتاً ایمن، ذاتاً اَمن و طراحی براساس تهدید، پیش بینی و تأمین تجهیزات، ملزومات و فناوری های مقابله با مخاطرات مانند؛ شبکه پایشگر مخاطرات، شبکه اطفاء حریق و رفع آلودگی و سایر،

۴ـ مدیریت و کاهش و خنثی سـازی مخاطرات مفـروض زیرساخت با طراحـی و پیاده سـازی عناصر، مولفه ها و اجـزاء طرح،

ماده۹ـ ساختار اجرایی

بمنظور راهبری و هدایت اجرای طرح راهبردی حفاظت از زیرساخت، سازمان با استفاده از ظرفیت های موجود خود و دستگاه های اجرایی نسبت به تشکیل شورای هماهنگی حفاظت از زیرساخت های با اهمیت بالا، کارگروه تنظیم مقررات حفاظت از زیرساخت های با اهمیت بالا و مرکز مدیریت و هماهنگی عملیاتی زیرساخت ها بشرح زیر، اقدام می کن د:

الف) شورای هماهنگی حفاظت از زیرساخت های با اهمیت بالا: به منظور سیاست گذاری و ایجاد هم گرایی، هم افزایی، مدیریت هماهنگ و رفع تعارض بین زیرساخت های حوزه های کلیدی در کشور، شورای هماهنگی حفاظت از زیرساخت های با اهمیت بالا درچارچوب این طرح با هدایت سازمان و عضویت متولیان اجرایی ۸ حوزه کلیدی و عناصر ذی ربط امنیتی و دستگاهی تشکیل می شود.

ب) کارگروه تنظیم مقررات حفاظت از زیرساخت های بااهمیت بالا: به منظور تدوین و تصویب ضوابط و مقررات حفاظت از زیرساخت های با اهمیت بالا، این کارگروه با هدایت سازمان و همکاری سازمان برنامه و بودجه کشور و سایر دستگاه های متولی حوزه های با اهمیت بالا و سازمان های امنیتی در سازمان تشکیل می شود.

ج) مرکز مدیریت و هماهنگی عملیاتی زیرساخت ها: این مرکز به منظور ایجاد هم گرایی، هم افزایی، هماهنگی و هدایت عملیاتی بین زیرساخت های با اهمیت بالای کشور در شرایط عادی و عملیات پدافندی (اضطراری) با ماموریت های زیر تشکیل می گردد و با دریافت اطلاعات از وضعیت موجود زیرساخت و تحلیل آن به لحاظ آسیب پذیری و تهدیدات و اشتراک گذاری و تبادل اطلاعات مرتبط با آنها اقدام می کند:

۱) رصد و پایش وضعیت زیرساخت ها از منظر تهدیدات، آسیب پذیری و آمادگی،

۲) راهبری، مدیریت و ارائه برنامه کاهش دائمی آسیب پذیری مشترک زیرساختی،

۳) بهینه سازی و مدیریت وابستگی متقابل بین زیرساختی،

۴) رفع تعارض و ایجاد هماهنگی و هم افزایی بین دستگاهی در ارائه مستمر خدمات زیرساختی،

۵) هدایت و راهبری عملیات پدافند غیرعاملی مشترک بین زیرساختی در شرایط پاسخ به حوادث و تهدیدات،

۶) برنامه ریزی هماهنگ و مشترک در جهت پاسخ هم گرا به حوادث و تهدیدات،

ماده۱۰ـ وظایف دستگاه های اجرایی

الف) وزارت راه و شهرسازی

۱) ملاحظات، الزامات، اصول و راهبردهای این طرح را در تهیه، بررسی و تصویب طرح های توسعه و عمران و طرح های کالبدی کشور اعمال و از اجرای آن اطمینان حاصل نموده و نتایج آن را هر ۶ ماه به سازمان گزارش کند.

۱-Cyber Emergency Response Plan

۲- Cyber Vulnerability Reduction Plan

۳- Cyber Business Countinuty Plan

۴- Cyber Disaster Recovery Plan

۵- Cyber Critical Infrastructure Protection Plan

۶- Cyber Preparedness Promotly Plan

۲) ملاحظات، الزامات، اصول و راهبردهای این طرح را در کلیه سطوح خدمات مهندسی اعم از مطالعه، طراحی، اجرا و نظارت، اعمال و پیاده سازی کند.

۳) توانمندسازی آموزشی و تخصّصی ظرفیت های فنی و مهندسی (حقیقی و حقوقی) متناسب با نیاز این طرح را با استفاده از ظرفیت های موجود در سازمان نظام مهندسی و کنترل ساختمان، اجرا کند.

۴) اجرای این طرح را با هماهنگی سازمان در قالب اصول و قواعد فنی لازم الرعایه حفاظت از زیرساخت ها در ضوابط و مقرّرات ملی ساختمان، پیاده سازی، توسعه و ترویج نماید.

۵) ضوابط و راهکارهای کاهش خطرپذیری و بهینه سازی استحکام ساختمان ها و ابنیه در برابر حوادث و تهدیدات را با هماهنگی سازمان تهیه، تصویب و ابلاغ کند.

۶) ملاحظات، الزامات، اصول و راهبردهای این طرح را در تهیه، بررسی و تصویب طرح های توسعه و عمران بنادر، فرودگاه ها، خطوط مواصلاتی شهری و بین شهری (ریلی، جاده ای، هوایی و دریایی) و خطوط ارتباطی با اهمیت بالای کشور اعمال و از اجرای آن اطمینان حاصل نموده و نتایج آن را به سازمان گزارش کند.

ب) وزارت دفاع و پشتیبانی نیروهای مسلح

۱) مرکز تدوین، تنظیم و روزآمدسازی ضوابط، مقرّراتِ فنی مهندسی حفاظت از زیرساخت های با اهمیت بالا را با استفاده از ظرفیت های موجود در دانشگاه صنعتی مالک اشتر با راهبری و هدایت سازمان تشکیل و راه اندازی کند.

۲) استانداردهای تخصّصی حفاظت از زیرساخت های بااهمیت بالا را جهت تصویب در کارگروه تنظیم مقرّرات حفاظت از زیرساخت، تدوین و تولید کند.

۳) نسبت به آموزش و تربیت نیروی انسانی متخصّص در مقاطع کارشناسی، کارشناسی ارشد و دکتری در حوزه حفاظت از زیرساخت ها و سایر رشته ـ گرایش های مرتبط بین رشته ای با هماهنگی سازمان اقدام کند.

۴) نسبت به پژوهش و تولید و مدیریت دانش تخصّصی حفاظت از زیرساخت ها و بومی سازی آن در نظام آموزشی ذی ربط اقدام کند.

۵) نسبت به پشتیبانی از زیرساخت های بااهمیت بالا شامل تجهیزات شناسایی، رصد و پایش تهدیدات، تولید تجهیزات تخصّصی پدافند غیرعامل، برابر راهبردهای این طرح اقدام کند.

۶) ملاحظات، الزامات، اصول و راهبردهای این طرح را در تهیه، بررسی و تصویب طرح های بخش دفاعی وزارت دفاع اعمال و از اجرای آن اطمینان حاصل نموده و نتایج آن را به صورت فصلی به سازمان گزارش کند.

ج) وزارت کشور

۱) در تهیه طرح های جامع امنیت از الزامات و ملاحظات این طرح به عنوان مکمل بخش امنیتی و دفاعی استفاده و در آن اعمال کند.

۲) ملاحظات، الزامات، اصول و راهبردهای این طرح را در تهیه، بررسی و تصویب طرح های جامع حمل و نقل و ترافیک شهرهای کشور اعمال و از اجرای آن اطمینان حاصل نموده و نتایج آن را به سازمان گزارش کند.

۳) هماهنگی لازم را با سازمان برای هدایت استانداران و فرمانداران و شهرداران در پیاده سازی اهداف و ماموریت های این طرح به عمل آورد.

۴) با تطبیق، کنترل و نظارت بر رعایت اصول و اجرای راهبردهای این طرح در پروژه ها و طرح های توسعه و عمران و طرح های کالبدی استانی و شهری کشور نسبت به پیاده سازی الزامات و ملاحظات و راهبردهای حفاظت از زیرساخت، در این سطوح اقدام کند.

۵) اجرای طرح حفاظت از زیرساخت های شهری را در قالب برنامه های توسعه شهری با ملاحظات مندرج در این طرح و سند راهبردی پدافند شهری ـ مصوبه شماره ۲۰۲۲ مورخ ۱۳۹۸/۹/۲۴ کمیته دائمی ـ راهبری و نظارت نماید.

د) وزارت ارتباطات و فناوری اطلاعات

۱) نسبت به افزایش تاب آوری، پایداری، مانورپذیری و حصول اطمینان از استمرار خدمات ضروری شبکه زیرساخت ارتباطی کشور در مقابل تهدیدات و حملات سایبری در تراز جنگ سایبری اقدام کند.

۲) نسبت به حفظ پایداری و استمرار خدمات اساسی سایبری مانند به روزرسانی نرم افزارهای پرکاربرد، سیستم عامل ها، ایجاد و به روز نگه داشتن مخازن۱ نرم افزارها، مجوزهای۲ نرم افزاری پرکاربرد، سامانه های نام دامنه۳، درجهت کاهش وابستگی کشور و بی اثرسازی اقدامات خصمانه دشمن در فضای سایبری اقدام کند.

۱- Repository

۲- Licence

۳- DNS

۳) نسبت به ارتقای پایداری خدمات پدافند و امنیت سایبری مانند توانمندسازی افراد، ایجاد، سازماندهی و عملیاتی کردن تیم های واکنش به رخدادهای سایبری ـ CERT۱ـ مدیریت وصله زنی۲ امنیتی، مقابله و کاهش حملات منع سرویس توزیع شده اقدام کند.

۴) نسبت به ایجاد شبکه های اختصاصی و محدود، اَمن و مطمئن برای ارتباط زیرساخت های با اهمیت بالا با رعایت اصول پدافند و امنیت سایبری اقدام کند.

۵) ملاحظات، الزامات، اصول و راهبردهای این طرح را در تهیه، بررسی و تصویب طرح های توسعه خطوط ارتباطات و فناوری اطلاعات کشور اعمال و از اجرای آن اطمینان حاصل نموده و نتایج آن را به صورت فصلی به سازمان گزارش نماید.

۶) الزامات و ملاحظات پدافند غیرعامل و اصول و راهبردهای حفاظت از زیرساخت های با اهمیت بالا را در کلان پروژه شبکه ملی اطلاعات پیاده سازی و اجرا کند.

هـ) وزارت علوم، تحقیقات و فناوری

۱) نسبت به طراحی رشته تحصیلی حفاظت از زیرساخت و برنامه ریزی جامع برای آموزش و تربیت نیروی انسانی متخصص در مقاطع کارشناسی،کارشناسی ارشد و دکتری در حوزه حفاظت از زیرساخت و سایر رشته ـ گرایش های مرتبط بین رشته ای با همکاری سازمان، اقدام کند.

۲) نسبت به ایجاد حداقل یک دانشکده تخصّصی در حوزه حفاظت از زیرساخت در یکی از دانشگاه های برتر کشور، با هماهنگی سازمان اقدام کند.

۳) با هدایت توانمندی هایِ مراکز رشد، شرکت های دانش بنیان، پارک های علم و فناوری تابعه و راه اندازی انجمن های علمی حفاظت از زیرساخت در دانشگاه های منتخب، نسبت به مطالعه، تدوین، تنظیم و به روزرسانی ضوابط، مقررات فنی ـ تخصصی حفاظت از زیرساخت در حوزه های کالبدی و سایبری اقدام کند.

۴) با استفاده از ظرفیت دانشگاه ها، مراکز پژوهشی و پارک های علم و فناوری نسبت به پژوهش و تولید و مدیریت دانش تخصّصی حفاظت از زیرساخت ها و بومی سازی آن در نظام آموزش عالی اقدام کند.

۵) راهبردهای این طرح را در زیرساخت های با اهمیت بالای خود از قبیل ازمایشگاه های مرجع، دانشگاه ها و پژوهشگاه های تخصصی، پارک های علم و فناوری و مانند ان پیاده سازی و اجرا کند.

و) سازمان برنامه و بودجه کشور

۱) الزامات، ملاحظات و مقررات فنی و اجرایی مصوب کارگروه تنظیم مقررات حفاظت از زیرساخت های با اهمیت بالا را در برنامه ها، طرح ها و پروژه های حیاتی، حساس و مهم کشور نهادینه سازی کرده و اجرای آنها را از طریق کمیسیون مصوبات طرح های عمرانی کنترل کرده و مصوبات خود را هر ۶ ماه به سازمان گزارش نماید.

۲) برای حصول اطمینان از اعمال ضوابط و مقررات پدافند غیرعامل در طرح ها و پروژه های حیاتی، حساس و مهم حوزه های با اهمیت بالای کشور در چارچوب نظام فنی و اجرایی کشور و با هماهنگی سازمان، ترتیبات لازم را در اجرای مواد ۴۰ و ۴۱ شرایط عمومی پیمان ـ تحویل موقت و دائمی طرح و صدور پایانِ کار ـ پیش بینی نماید.

۳) در تدوین و تصویب برنامه ملی، بخشی، منطقه ای و استانی آمایش سرزمین و تصویب طرح های توسعه عمران و کالبدی کشور، ملاحظات راهبردی این طرح شامل کاهش مستمر آسیب پذیری ها، ارتقاء تاب آوری ملی، کاهش و بهینه سازی وابستگی متقابل راهبردی بین دستگاهی و تضمین تداوم کارکردهای اساسی کشور رعایت شود.

۴) چنانچه طرحی پس از اخذ مصوبه کمیسیون طرح های عمرانی (کمیسیون ماده۲۳ مقررات مالی دولت) بنا بر گزارش رئیس سازمان، ضوابط و مقررات پدافند غیرعامل را در هر مرحله از اجرای طرح رعایت نکند، اجرای طرح متوقّف و تخصیص بعدی اعتبارات اجرای آن طرح، منوط به اخذ تائیدیه سازمان خواهد بود.

ز) سپاه پاسداران انقلاب اسلامی ـ دانشگاه جامع امام حسین (ع)

۱) مرکز تدوین، تنظیم و به روزرسانی ضوابط، مقررات فنی مهندسی حفاظت سایبری از زیرساخت های سایبری و وابسته به فضای سایبر با اهمیت بالا کشور را در ساختار دانشگاه جامع امام حسین(ع) با راهبری و هدایت سازمان تشکیل و راه اندازی کند.

۲) نسبت به آموزش و تربیت نیروی انسانی متخصّص در مقاطع کارشناسی، کارشناسی ارشد و دکتری در حوزه حفاظت از زیرساخت ها و سایر رشته ـ گرایش های مرتبط بین رشته ای اقدام کند.

۳) نسبت به پژوهش و تولید و مدیریت دانش تخصصی حفاظت از زیرساخت ها و بومی سازی آن در نظام آموزشی ذی ربط اقدام کند.

۱- Computer Emergency Response Team

۲- Patch management

ح) وزارت اطلاعات و سازمان اطلاعات سپاه

۱) نسبت به مدیریت و کاهش تهدیدات درون زا در دستگاه های اجرایی اقدام و از آسیب ناپذیری یا حداقل آسیب پذیری ممکن اطلاعاتی و ضد اطلاعاتی زیرساخت های با اهمیت بالا اطمینان حاصل نماید.

۲) نسبت به رصد، پایش، تشخیص، برآورد و هشدار تهدیدات و آسیب پذیری ها و مخاطرات زیرساختی و اشتراک اطلاعاتی بین ذی نفعان اقدام کند.

۳) ضمن تأمین، برآورد و اشراف اطلاعاتی مربوط به تهدیدات زیرساخت های با اهمیت بالا، در اجرای عملیات پدافند غیرعامل زیرساختی، پشتیبانی اطلاعاتی لازم از سازمان به عمل آورند.

تبصره: اجرای ماموریت های فوق در چارچوب ماموریت های سازمانی مصوب و با حداکثر هماهنگی با سازمان در زمان وقوع تهدیدات در جهت کسب اشراف اطلاعاتی و اقدام بی درنگ، مورد تاکید و اقدام است.

ط) سازمان مناطق آزاد تجاری ـ صنعتی و مناطق ویژه اقتصادی کشور موظف است الزامات و ملاحظات این طرح و دستورالعمل های مربوط به آن را در طرح های جامع و کالبدی خود اعم از طرح های جدید و زیرساخت های موجود در مراحل مختلف (طراحی، ساخت و اجرا، بهره برداری) رعایت نموده و آخرین وضعیت پیاده سازی اجرای این طرح را بصورت فصلی به سازمان، گزارش کند.

ی) سازمان پدافند غیرعامل کشور

۱) مباحث حفاظت از زیرساخت را با همکاری سازمان برنامه و بودجه کشور و دفتر مقررات ملی ساختمان، در زیرساخت های با اهمیت بالا و شریان های حیاتی مانند بنادر، فرودگاه ها، خطوط راه آهن و مانند آن، ظرف مدت یک سال، تدوین و تصویب کند.

۲) نظام فنی ـ تخصّصی حفاظت از زیرساخت های کشور را پس از ۶ ماه از تاریخ ابلاغ این طرح، تهیه و ابلاغ کند.

۳) دستورالعمل حفاظت از زیرساخت های وابسته به سایبری را در برابر تهدیدات سایبری و الکترونیک و الکترو مغناطیس را با مشارکت و همکاری دستگاه های اجرایی ذی ربط ظرف مدت یک سال، تهیه و ابلاغ کند.

۴) به منظور حصول اطمینان از اِعمال الزامات و مقرّرات پدافند غیرعامل در طرح های زیرساختی کشور نظام نظارت، کنترل فنی و صدور پایانِ کار پدافند غیرعامل طرح ها و پروژه های جدید و با اهمیت بالای کشور را تهیه و ابلاغ نمودَه و نتیجه اجرای آن را هر ۶ ماه به کمیته دائمی گزارش کند.

۵) به منظور حصول اطمینان از آمادگی زیرساخت های با اهمیت بالا در برابر تهدیدات مفروض، اجرای رزمایش های پدافند کالبدی و سایبری در مراکز حیاتی، حساس و مهم را به طور نوبه ای ارزیابی و کنترل نماید.

ماده۱۱ـ اقدامات مشترک دستگاه های اجرایی

کلیه دستگاه های اجرایی مشمول، موظّف به اجرای موارد زیر می باشند:

۱) بازنگری و بازمهندسی نظام سطح بندی براساس مولفه های تعیین شده با قابلیت به روزرسانی دوره ای و اخذ تاییدیه سازمان،

۲) تدوین، طراحی و پیاده سازی نظام عملیاتی روزآمد تداوم کارکرد و بازیابی در قالب زیرساخت ها و شریان های منعطف، مقاوم و تاب آور در برابر تهدیدات و حوادث،

۳) تهیه، بازنگری، به روز رسانی و پیاده سازی طرح های عملیاتی حفاظت فیزیکی و سایبری از زیرساخت های حیاتی، حساس و مهم خود اعم از:

۱ـ طرح پاسخ اضطراری به حوادث و تهدیدات زیرساختی،

۲ـ طرح تضمین و تسهیل تداوم کارکردهای اساسی،

۳ـ طرح بازیابی و برگشت پذیری زیرساختی،

۴ـ طرح اَمن سازی و مصون سازی زیرساختی،

۵ ـ طرح کاهش آسیب پذیری های زیرساختی،

۶ ـ طرح ارزیابی و ارتقاء آمادگی های زیرساختی،

۷ـ طرح بهینه سـازی وابستگی و وابستگی های متقابل زیرساختی،

۴) ذخیره سازی، موازی سازی، اَمن سازی، جایگزینی خدمات، تطبیق پذیری با تمرکز بر برطرف نمودن یا موازی نمودن گره های زنجیره تولیدات و خدمات زیرساخت ها،

۵) ایجاد سامانه یکپارچه برای رصد، پایش، ارزیابی، تشخیص و هشداردهی روزآمد تهدیدات و آسیب پذیری ها در زیرساخت ها و شریان های حیاتی،

۶) تدوین و پیاده سازی برنامه عملیاتی مدیریت و کاهش تهدیدات درون زا در زیرساخت های با اهمیت بالا،

۷) تهیه، تدوین، اجرا و پیاده سازی نظام عملیاتی مصون سازی سایبری در زیرساخت های با اهمیت سایبری و وابسته به سایبر،

۸) اجرای برنامه های آموزشی منسجم و رزمایش هدفمند ارتقاء آمادگی و توانمندسازی مدیران و کارشناسان فعال در مراکز و زیرساخت های حیاتی، حساس و مهم متناسب با طرح های عملیاتی پدافندی زیرساختی،

۹) پیاده سازی رویکرد انتقال اقدامات و برنامه های پدافند غیرعاملی حفاظت از زیرساخت از پیوست به ذات طرح های توسعه زیرساختی در مراحل مطالعه و طراحی،

۱۰) تدوین و نهادینه سازی برنامه های مصون سازی تخصصی و مدیریت مخاطرات در زیرساخت های پرخطر،

۱۱) تبادل اطلاعات مخاطرات و تهدیدات زیرساختی با دستگاه ها و نهادهای امنیتی و اطلاعاتی،

۱۲) تهیه و تدوین طرح حفاظت از زیرساخت مراکز حیاتی، حساس و مهم خود ـ SSP۱ ـ ظرف یک سال از ابلاغ این طرح،

۱۳) تهیه گزارش سالانه و روزآمد شامل برآورد تهدیدات، آسیب پذیری ها، وابستگی های متقابل و مخاطرات و اقدامات انجام شده هر دستگاه در برابر آنها همراه با تجزیه و تحلیل و ارسال به سازمان،

ماده۱۲ـ استانداردها، الزامات و ملاحظات عمومی و تخصّصی پدافند غیرعامل حفاظت از زیرساخت های موجود و جدید حوزه های با اهمیت بالای کشور توسط سازمان تهیه، تنظیم و ابلاغ می شود و برای دستگاه های اجرایی و بخش خصوصی، لازم الاجراست.

ماده۱۳ـ به منظور حصول اطمینان از رعایت الزامات و ملاحظات پدافند غیرعامل در اجرای طرح های عمرانی و زیرساخت های جدید (حیاتی، حساس و مهم) دستگاه های اجرایی موظّف به انجام آزمون پایداری طرح در برابر تهدیدات براساس طرح پایه، صحت سنجی اجرای طرح حفاظت از زیرساخت و اخذ تائیدیه پدافند غیرعامل از سازمان، جهت صدور پایانِ کار می باشند.

ماده۱۴ـ حفاظت از اطلاعات و اسناد پدافند غیرعامل زیرساخت های با اهمیت بالا در اشکال مختلف آن از قبیل سند کتبی و پوشه الکترونیکی چند رسانه ای و مانند آنها، در کلیه مراحل اجرای طرح، وفق مصوبه شماره ۱۶۰/۱/۸۰۴ مورخ ۱۳۹۴/۱۱/۱۴ کمیته دائمی و ابلاغیات سازمان حراست کل کشور، لازم الاجراست.

ماده۱۵ـ اعتبار موردنیاز برای اجرای این طرح در زیرساخت های جدید براساس ساز وکار پیش بینی شده در قوانین از جمله ماده۲۳ قانون الحاق برخی مواد به قانون تنظیم بخشی از مقررات مالی دولت(۲) و از محل اعتبارات اجرای همان طرح، تأمین می شود و اعتبار موردنیاز برای زیرساخت های درحال بهره برداری، براساس مطالعات و برآوردهای انجام شده توسط دستگاه اجرایی، در اعتبارات سالانه دستگاه، پیش بینی و تأمین می گردد؛ بخش خصوصی و شرکت های غیردولتی دارای زیرساخت های با اهمیت بالا ملزم به تأمین اعتبار مورد نیاز اجرای طرح حفاظت از زیرساخت خود از منابع داخلی می باشند.

ماده۱۶ـ سازمان با همکاری دستگاه های اجرایی ذی ربط، دستورالعمل ها و طرح های اجرایی موردنیاز برای پیاده سازی این طرح را تهیه و به دستگاه های اجرایی ابلاغ می کند.

ماده۱۷ـ دستگاه های اجرایی موظفند هرگونه قصور و کوتاهی در اجرای این طرح در زیرساخت های حوزه های با اهمیت بالا را به سازمان گزارش کرده و برابر مقررات با فرد متخلّف، برخورد کنند.

ماده۱۸ـ سازمان با مستنکفین از این طرح بنابر تخلّف صورت گرفته و براساس شیوه نامه ای که توسط سازمان تنظیم و ابلاغ می گردد برخورد انضباطی کرده و در صورت نیاز از طریق قوه قضائیه اقدام می کند.

ماده۱۹ـ سازمان بر حسن اجرای این طرح، نظارت و اجرای آن را بصورت سالانه به کمیته ی دائمی گزارش کند.

ماده۲۰ـ طرح راهبـردی حفاظت از زیرسـاخت های کشور در بیست مادّه و دو تبصره در تاریخ بیست ونهم شهریورماه سال یکهزار و چهارصد و یک هجری شمسی در شصت و ششمین جلسه کمیته دائمی به تصویب رسید.

طرح راهبـردی حفاظت از زیرسـاخت های کشور مشتمل بر بیست مـادّه و دو تبصره که در تاریخ ۲۹/ ۰۶/ ۱۴۰۱ در شصت وششمین جلسه کمیته دائمی(شورای عالی) پدافند غیرعامل کشور به تصویب رسید، به استناد تبصره یک ماده نه اساسنامه سازمان پدافند غیرعامل کشور مصوب مقام معظّم رهبـری و فرماندهی کل قـوا (مدظله العالی) جهت اجرا ابلاغ می گردد.

رئیس ستاد کل نیروهای مسلح و کمیته دائمی پدافند غیرعامل کشور

سرلشکر پاسدار محمّد باقری

۱- Sector Specific Plan

چاپ قانون