جمهوری اسلامی ایران

فرماندهی کل قوا

کمیته دائمی پدافند غیرعامل کشور

شماره: ۱۶۰/۱/۲۳۰۱

تاریخ: ۱۴۰۱/۰۷/۲۰

پیوست: ندارد

بسم الله الرحمن الرحیم

مقام معظم رهبری و فرماندهی کل قوا (مدظله العالی):

« 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 تو طئه 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. »

تصویب‌نامه

وزیر محترم کشور

وزیر محترم دفاع و پشتیبانی نیروهای مسلّح

معاون محترم رئیس جمهور و رئیس سازمان برنامه و بودجه کشور

رئیس محترم کمیسیون امنیّت ملّی و سیاست خارجی مجلس شورای اسلامی

سردار معاون محترم هماهنگ کننده ستادکل نیروهای مسلّح

سردار رئیس محترم سازمان پدافند غیرعامل کشور

سلامٌ علیکم

باصلوات برمحمد وآل محمد و احترام؛ به استناد ماده۸ اساسنامه سازمان پدافند غیرعامل کشور مصوّب مقام‌معظّم رهبری و فرماندهی کلّ قوا (مدظله‌العالی) در تاریخ ۱۴۰۱/۰۶/۲۹ شصت‌وششمین جلسه کمیته‌دائمی (شورای‌عالی) پدافند غیرعامل کشور تشکیل و طرح‌راهبردی‌حفاظت از زیرساخت‌های‌کشور موضوع مادّه نه اساسنامه، پیشنهادی آن سازمان را بررسی و به‌شرح‌زیر تصویب‌نمود؛

طرح راهبردی حفاظت از زیرساخت‌های کشور

مقدمه

زیرساخت‌های هر کشور، بستر مهم حیات، رشد و پویایی آن به‌شمار می‌رود، برخی از زیرساخت‌ها نقشی حیاتی در حفظ منافع ملی دارند و بعنوان یکی از ارکان مهم پیشرفت، اختلال هرچند کوتاه‌مدت در عملکرد آنها می‌تواند منجر به آسیب جدی در اقتصاد و امنیت ملی شود؛ از آنجا که زیرساخت‌ها، جریانی به‌هم پیوسته از خدمات و پشتیبانی‌ها را برای تأمین نیازهای اساسی به جامعه ارائه می‌دهند و آسیب یا اختلال در عملکرد و کارکرد آنها می‌تواند قطع خدمات زیرساختی به مردم و جامعه را در پی داشته باشد؛ از این رو طرح راهبردی حفاظت از زیرساخت‌های کشور، به عنوان عالی‌ترین سند پدافند کالبدی و حفاظت از زیرساخت‌های کشور، در راستای مصون‌سازی زیرساخت‌ها و شریان‌های حیاتی و حفظ و تضمین تداوم ارائه خدمات ضروری به بخش‌های مختلف جامعه و مردم تدوین شده است.

ماده۱– تعاریف و اختصارات

۱) **سازمان:** سازمان پدافند غیرعامل کشور

۲) **کمیته دائمی:** کمیته دائمی پدافند غیرعامل کشور

۳) **زیرساخت[1]:** به مجموعه‌ای از مراکز و تأسیسات زیربنایی و شریان‌های عمده که خدمات و نیازهای ضروری و اساسی کشور را به مردم و جامعه ارائه می‌کند، اطلاق می‌گردد؛ زیرساخت مشتمل بر فرابخش[2](حوزه)، بخش[3]، زیربخش[4]، دارایی[5] و اجزاء آن می‌باشد.

۴) **حوزه‌های با اهمیت بالا[6]:** به هریک از حوزه‌های ۱- انرژی، ۲-آب، ۳- غذا و کشاورزی، ۴ - حمل و نقل، ۵- بهداشت و سلامت، ۶- دفاعی و امنیتی، ۷- صنعت، ۸- رسانه، ۹- هسته‌ای، ۱۰- فضا، ۱۱- جمعیت، ۱۲- حاکمیتی، ۱۳- خدمات ضروری و فوریتی، ۱۴- پولی و مالی، ۱۵- ارتباطات و فناوری اطلاعات، حوزه‌های با اهمیت بالا گفته می‌شود که باتوجه به شاخص‌های زیر، حوزه‌های؛ **۱- انرژی، ۲- آب، ۳- ارتباطات و فناوری اطلاعات، ۴- حمل‌ونقل، ۵- بهداشت و سلامت، ۶- غذا و کشاورزی، ۷- دفاعی و امنیتی** و **۸- حاکمیتی** بعنوان حوزه‌های کلیدی از منظر پدافند غیرعامل دسته‌بندی می‌شوند:

- اهمیت کارکرد هر حوزه در تأمین نیازهای حیاتی مردم در شرایط اضطراری
- شدت اثرگذاری بر اقتصاد، امنیت ملی و سلامت مردم
- وابستگی زیرساخت‌های سایر حوزه‌ها 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 زیرساخت‌ها موجب تولید بازدارندگی، کاهش آسیب‌پذیری، تسهیل مدیریت بحران، ارتقاء تاب‌آوری زیرساختی، آمادگی پاسخ پدافندی به تهدید، پایداری و مصونیت‌بخشی، مدیریت مخاطرات و تضمین تداوم کارکرد و استمرار خدمات اساسی در برابر تهدیدات و اقدامات نظامی دشمن می‌شود.

۶) **طرح راهبردی:** مجموعه‌ای یکپارچه متشکل از مطلوبیت‌های راهبردی از قبیل اصول، ارزش، ماموریت، اهداف کلان و چشم‌انداز، راهبردها، اقدامات اساسی، برنامه‌ها، راهبردهای عملیاتی و الزامات تحقق آنهاست که پیاده‌سازی آن می‌تواند دستیابی به اهداف را تسهیل کند.

۷) **حفاظت از زیرساخت[7]:** مجموعه تدابیر و اقدامات پدافند غیرعاملی که توانایی و آمادگی عملیاتی زیرساخت و تداوم کارکردهای آن و دستگاه‌های 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 می‌دهد بطوری‌که فعالیّت آن حفظ گردیده و خسارات انسانی و مادی ناشی از آن را به حداقل می‌رساند.

۸) **مخاطره امنیتی – نظامی:** به اندرکنش تهدیدات با آسیب‌پذیری‌ها و احتمال وقوع و شدت پیامد آنها با منشاء دشمن در حوزه‌های زیستی، سایبری، شیمیایی، پرتوی، تروریستی، امنیتی، نظامی و یا ترکیبی از آنها که با هدف ضربه‌زدن به امنیت ملی کشور باشد، اطلاق می‌گردد.

۹) **تهدیدات درون زا[8]:** به تهدیداتی اطلاق می‌گردد که توسط کارکنان یک سازمان یا شبکه‌های همکار(پیمانکاران و سایرین) به صورت فردی یا شبکه‌ای، 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 می‌تواند شامل سرقت اطلاعات و فنآوری، خسارت به تأسیسات، سیستم‌ها، تجهیزات، کارکردها و فرآیندها، صدمه به کارمندان، توقّف فعالیت‌های ضروری و یا اقدامات دیگری در جهت صدمه‌زدن به مأموریت سازمان و منافع آن باشد.

۱۰) **مراکز ضروری:** مراکز و تاسیساتی که فقدان یا اختلال در عملکرد آنها زندگی مردم را با چالش مواجه می‌سازد.

۱۱) **شریان‌های اصلی و حیاتی:** به شبکه‌های زیرساختی و ارتباطی که نقش اصلی و حیاتی در تامین نیازهای اساسی اداره کشور و امور مردم را دارند اطلاق می‌شود؛ مانند شبکه‌های ارتباطات، آب و گاز و سایر.

1- Infrastructure 2- Sector 3- system 4- subsystem 5- Asset & components 6- Critical infrastructure 7- infrastructure protection 8- Insider threat

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 می‌شود.

۱۳) **سطح‌بندی:** میزان ارزش و اهمیت مراکز، تاسیسات و زیرساخت‌های کشور است که از منظر پدافند غیرعامل در سطوح حیاتی، حساس، مهم و قابل حفاظت تقسیم‌بندی و تعریف می‌شوند.

۱۴) **روابط سیستمی زیرساختی:** روابط حاکم بر زیرساخت‌ها مبتنی بر رویکرد سیستم از سیستم[1] و تعامل بین اجزای سیستم زیرساختی که منجر به ایجاد روابط سیستمی از قبیل هم‌افزایی، تضاد، وابستگی و وابستگی متقابل می‌شود.

۱۵) **آسیب‌پذیری[2]:** میزان خسارات و صدماتی است که از عوامل و پدیده‌های بالقوه (تهدیدات) یا بالفعل خسارت‌زا به نیروی انسانی، تجهیزات و تأسیسات با شدت صفر تا صددرصد ناشی می‌گردد.

۱۶) **تاب‌آوری[3]:** به توانایی یک نظام، جامعه، دستگاه اجرایی و یا زیرساخت برای ایستادگی، تحمّل، انعطاف‌پذیری و حفظ کارکرد، تطبیق و برگشت‌پذیری در برابر مخاطره امنیتی - نظامی گفته می‌شود.

۱۷) **تداوم کارکرد[4]:** توانایی ادامه تولید محصولات یا ارائه خدمات توسط زیرساخت‌ها در چارچوب زمانی مورد پذیرش، قابل‌قبول و درحد ظرفیت از پیش تعیین شده، حین و پس از وقوع مخاطره امنیتی- نظامی، تداوم کارکرد گفته می‌شود.

ماده۲- اسناد بالادستی

۱) فرامین، تدابیر و منویات مقام معظم رهبری (مدظله العالی)
۲) سیاست‌های کلی نظام در موضوع پدافند غیرعامل و آمایش سرزمین
۳) قانون احکام دائمی برنامه‌های توسعه کشور- ماده ۵۸
۴) سند جهت‌گیری‌های ملّی آمایش سرزمین - بندهای ۸۰ ، ۸۱ و ۸۲ از ماده ۱
۵) اساسنامه سازمان پدافند غیرعامل کشور
۶) قانون برنامه پنجساله ششم توسعه جمهوری اسلامی ایران - بند پ ماده ۱۰۶
۷) سیاست‌های کلی برنامه پنجساله هفتم توسعه جمهوری اسلامی ایران - بند ۲۴

ماده۳- منظور

۱) ایجاد درک مشترک از مفهوم حفاظت از زیرساخت، تعیین راهبردها، سیاست‌ها و وظایف اصلی دستگاه‌های اجرایی متولی حوزه‌های کلیدی برای دستیابی به اهداف پدافند کالبدی در کشور،
۲) تبیین چارچوبی مدوّن برای تهیه و تنظیم ضوابط و مقررات حفاظت از زیرساخت، برنامه‌های مصون‌سازی و ارتقاء آمادگی زیرساخت‌های حوزه‌های با اهمیت بالا و شریان‌های اصلی و حیاتی کشور،
۳) ایجاد هماهنگی، هم‌سویی و هم‌افزایی بین سازمان و دستگاه‌های اجرایی متولی حوزه‌های بااهمیت بالای کشور در راستای حفظ و ارتقاء پایداری ملی در شرایط اضطراری ناشی از وقوع تهدید،

ماده۴- حوزه شمول و حدود کاربرد طرح

الف) دستگاه‌های اجرایی متولی زیرساخت‌های حیاتی، حساس، مهم و قابل حفاظت (زیرساخت‌های دردست مطالعه، اجرا، ساخت و درحال بهره‌برداری) در هر یک از حوزه‌های با اهمیت بالای کشور
ب) سازمان‌های نیروهای مسلح دارای زیرساخت‌های صنعتی- اقتصادی مانند؛ نیروگاه، پالایشگاه و سایر
ج) بخش خصوصی و غیردولتی دارای زیرساخت‌های حیاتی، حساس، مهم و قابل حفاظت در حوزه‌های با اهمیت بالا
د) حدود کاربرد طرح در سلسله مراتب طرح‌های پدافند کالبدی زیر است:
۱) طرح‌های پدافند کالبدی زیرساخت دستگاهی: مطالعات پدافند غیرعامل زیرساخت‌های حوزه شمول (ماده۴ این طرح)

1-System of system 2- Vulnerability 3- Resiliency 4- Business continuity

۲) طرح‌های پدافند غیرعامل شهری: مطالعات پدافند غیرعامل زیرساخت‌های شهری
۳) طرح‌های جامع پدافند غیرعامل استانی: طرح‌ها و برنامه‌های پدافند غیرعامل استان و شهرستان
۴) طرح‌های جامع موضوعی پدافند کالبدی و حفاظت از زیرساخت کشور: طرح‌های راهبردی و ملی در موضوعات اساسی زیرساختی کشور مانند طرح جامع پدافند غیرعامل حفاظت از زیرساخت-SSP[1]- آب، برق، گاز و پتروشیمی
۵) طرح راهبردی و ملی حفاظت از زیرساخت‌ها و شریان‌های حائز اهمیت کشور

ماده ۵- اصول و ارزش‌ها

۱) اقتدار ذاتی و درون‌زای 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) تاب‌آوری زیرساختی
۸) تداوم کارکرد زیرساختی و خدمات ضروری
۹) تناسب اهمیت با امنیت زیرساخت
۱۰) کاهش مستمر آسیب‌پذیری
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- فایده)
۱۶) تقدّم امنیت بر توسعه
۱۷) پدافند عمیق و لایه به لایه
۱۸) توسعه‌ی امنیت افزا و ذاتاً اَمن
۱۹) حفظ سرمایه‌های ملی

ماده ۶- تهدیدات مفروض

تهدیدات مفروض این طرح عبارتند از:
۱) تهدیدات نظامی (هوایی، زمینی، دریایی، موشکی)
۲) تهدیدات امنیتی و تروریستی (اقدامات ضدزیرساختی تروریستی)
۳) تهدیدات سایبری زیرساختی (تهدیدات زیرساختی سایبری علیه زیرساخت‌های 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 می‌شود.

ماده۷- اهداف و مأموریت‌های عمده

اهداف و مأموریت‌های عمده در طرح راهبردی حفاظت از زیرساخت‌های کشور عبارت است از:
۱) سطح‌بندی روزآمد زیرساخت‌ها و دارایی‌های حوزه‌های با اهمیت بالا،
۲) رصد و پایش، تشخیص، هشدار و مدیریت تهدیدات زیرساختی،
۳) مصون‌سازی، اَمن‌سازی، تاب آور نمودن زیرساخت‌ها متناسب با سطح اهمیت آنها،
۴) تضمین و تسهیل تداوم کارکرد و استمرار خدمات ضروری زیرساخت‌های حیاتی در کشور،
۵) بهینه‌سازی سطح وابستگی و کاهش مستمر آسیب‌پذیری در زیرساخت‌ها متناسب با سطح اهمیت آن‌ها،
۶) نهادینه‌سازی اصول و الزامات پدافند غیرعامل در ذات طرح‌های توسعه زیرساختی کشور،
۷) کاهش و خنثی‌سازی درونی و ذاتی مخاطرات زیرساخت‌های دارای پتانسیل خطر در زمان طراحی و ساخت،
۸) مصونیت زیرساخت‌های سایبری و وابسته به سایبر و هوشمند،

1- Sector Specific Plan

۹) پاسخ به حوادث و تهدیدات و ایجاد آمادگی در برابر آنها در زیرساخت‌های حوزه‌های با اهمیت بالا،
۱۰) مدیریت و کاهش تهدیدات درون‌زا در زیرساخت‌های حوزه‌های با اهمیت بالا،
۱۱) توانمندسازی و آموزش مدیران و کارکنان دستگاه‌های متولی راهبری زیرساخت‌های حوزه‌های با اهمیت بالا،
۱۲) هماهنگی حداکثری و هم‌افزایی دستگاهی برای ارتقاء آمادگی‌های عملیاتی و تداوم کارکردهای ضروری،

ماده ۸– راهبردها

۱) سطح‌بندی زیرساخت‌ها مبتنی بر مؤلفه‌های ماهیت، اهمیت، هوشمندی، کارکرد، سیستمی یا غیرسیستمی بودن و خطرزایی با نظام روزآمد سطح‌بندی زیرساخت‌ها و دارایی‌ها،
۲) نهادینه‌سازی اصول، الزامات و ملاحظات حفاظت از زیرساخت در ذات طرح‌های توسعه زیرساخت در برابر انواع تهدیدات (مهاجرت پدافند از پیوست به ذات طرح) از طریق:
۱– مصون‌سازی در لایه طرح‌های پایه با چارچوب‌های فنی و مهندسی با رعایت اندرکنش سیستمی زیرساخت‌ها
۲– مصون‌سازی با تاکید بر انتخاب فناوری موردنیاز طرح و پیش‌بینی الزامات پدافندی در ذات فناوری و طرح
۳) توسعه و پیاده‌سازی سامانه رصد، پایش، ارزیابی، تشخیص و هشداردهی روزآمد تهدیدات و آسیب‌پذیری‌ها در زیرساخت‌ها و شریان‌های حیاتی و شبکه‌سازی آن در قالب سامانه یکپارچه ملی،
۴) ارتقاء امنیت و پایداری زیرساخت‌ها و شریان‌های حیاتی کشور با تهیه طرح‌های جامع عملیاتی پدافندی در جهت مصون‌سازی، افزایش آمادگی، ارتقاء تاب‌آوری و اَمن‌سازی اضطراری- EOP[1] با رویکرد زیست بوم، متمرکز بر اقدامات اساسی زیر:
۱– تهیه و پیاده‌سازی طرح پاسخ اضطراری به حوادث و تهدیدات زیرساختی- ERP[2]
۲– تهیه و پیاده‌سازی طرح تضمین و تسهیل تداوم کارکردهای اساسی- BCP[3]
۳– تهیه و پیاده‌سازی طرح بازیابی و برگشت‌پذیری زیرساختی و سیستمی- DRP[4]
۴– تهیه و پیاده‌سازی طرح اَمن‌سازی و مصون‌سازی و تاب‌آوری- ISP[5]
۵– تهیه و پیاده‌سازی طرح کاهش آسیب‌پذیری- VRP[6]
۶– تهیه و پیاده‌سازی طرح بهینه‌سازی وابستگی و وابستگی‌های متقابل- OIP[7]
۷– تهیه و پیاده‌سازی طرح‌های ارزیابی و ارتقاء آمادگی‌های زیرساختی- PPP[8]
۵) حفظ و تداوم کارکردهای ضروری و تأمین نیازهای اساسی کشور از طریق طراحی، پیاده‌سازی و روزآمدسازی نظام عملیاتی حفظ و تداوم کارکرد زیرساخت‌ها،
۶) پایدارسازی و تاب‌آور نمودن زیرساخت‌های حیاتی با قابلیت برگشت‌پذیری سریع، انعطاف‌پذیر 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) بهینه‌سازی وابستگی متقابل در زیرساخت‌های حیاتی کشور از طریق ذخیره‌سازی، اَمن‌سازی، جایگزینی خدمات، تطبیق‌پذیری با تمرکز بر برطرف نمودن یا موازی نمودن گره‌های زنجیره تولیدات و خدمات،
۸) استفاده حداکثری از ظرفیت‌های دستگاهی با تاکید بر تداوم کارکرد زنجیره فعالیت /خدمت از طریق نقش پذیری مناسب دستگاه‌های ذی نقش با هماهنگی و هم‌افزایی دستگاهی و مدیریت و فرماندهی یکپارچه،
۹) طراحی، پیاده‌سازی نظام، ساختار و الزامات تحقق برنامه کاهش مستمر تهدیدات درون‌زا با رصد و مراقبت نوبه‌ای،

1- Emergency operations Plan 2- Emergency Response Plan 3- Business Countinuty Plan 4- Disaster Recovery Plan 5- Immunius & Security Plan
6- Vulnerability Reduction Plan 7-Optimizing Interdependency Plan 8- Preparedness Promotly Plan

۱۰) مصون‌سازی سایبری همه‌جانبه، چندلایه و تطبیق‌پذیر زیرساخت‌های حائز اهمیت سایبری و وابسته به سایبر کشور در مقابل تهدیدات سایبری دشمن از طریق:

۱- شناسایی و ارزیابی دارایی‌های سایبری و تعیین سطح اهمیت آنها،
۲- رصد، پایش، برآورد تهدیدات و اشتراک‌گذاری اطلاعات،
۳- رفع یا کاهش آسیب‌پذیری‌های سایبری دارایی‌های سایبری و وابسته به سایبر،
۴- برآورد، تحلیل و مدیریت مخاطرات سایبری زیرساخت و پیامدهای آبشاری آن،
۵- نظام‌مند کردن ساختار امنیت و پدافند سایبری و فرآیندها و نیروی انسانی،
۶- روزآمدسازی و بومی‌سازی هوشمندی در زیرساخت‌های حیاتی کشور وابسته به فضای سایبر،
۷- حفاظت سایبری از زیرساخت‌های وابسته به فضای سایبر با تهیه و پیاده‌سازی طرح‌های عملیاتی پدافند سایبری - CERP[1],CVRP[2],CBCP[3],CDRP[4],CCIP[5],CPPP[6]

۱۱) ارتقاء آمادگی حداکثری و توانمندسازی مدیران و کارشناسان دستگاه‌های متولی راهبری حوزه‌های با اهمیت بالا با تاکید برتجهیز، تمرین، رزمایش، ارتقاء آمادگی و بازخورد و اصلاح طرح‌های عملیاتی پدافندی و رزمایش‌های تخصصی،

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

۱- سطح‌بندی زیرساخت‌ها از منظر خطرپذیری،
۲- آمادگی و پاسخ دائمی به حوادث و رخدادها و مخاطرات،
۳- بهره‌گیری از رویکرد طراحی و مصون‌سازی تخصصی در ذات طرح مبتنی بر طراحی ذاتاً ایمن، ذاتاً آمن و طراحی براساس تهدید،پیش‌بینی و تأمین تجهیزات، ملزومات و فناوری‌های مقابله با مخاطرات مانند؛ شبکه پایشگر مخاطرات، شبکه اطفاء حریق و رفع آلودگی و سایر،
۴- مدیریت و کاهش و خنثی‌سازی مخاطرات مفروض زیرساخت با طراحی و پیاده‌سازی عناصر، مولفه‌ها و اجزاء طرح،

ماده ۹- ساختار اجرایی

بمنظور راهبری و هدایت اجرای طرح راهبردی حفاظت از زیرساخت، سازمان با استفاده از ظرفیت‌های موجود خود و دستگاه‌های اجرایی نسبت به تشکیل شورای هماهنگی حفاظت از زیرساخت‌های با اهمیت بالا، کارگروه تنظیم مقررات حفاظت از زیرساخت‌های با اهمیت بالا و مرکز مدیریت و هماهنگی عملیاتی زیرساخت‌ها بشرح زیر، اقدام می‌کند:

الف) شورای هماهنگی حفاظت از زیرساخت‌های با اهمیت بالا : به منظور سیاست‌گذاری و ایجاد هم‌گرایی، هم‌افزایی، مدیریت هماهنگ و رفع تعارض بین زیرساخت‌های حوزه‌های کلیدی در کشور، شورای هماهنگی حفاظت از زیرساخت‌های با اهمیت بالا درچارچوب این طرح با هدایت سازمان و عضویت متولیان اجرایی ۸ حوزه کلیدی و عناصر ذی‌ربط امنیتی و دستگاهی تشکیل می‌شود.

ب) کارگروه تنظیم مقررات حفاظت از زیرساخت‌های بااهمیت بالا : به منظور تدوین و تصویب ضوابط و مقررات حفاظت از زیرساخت‌های با اهمیت بالا، این کارگروه با هدایت سازمان و همکاری سازمان برنامه و بودجه کشور و سایر دستگاه‌های متولی حوزه‌های با اهمیت بالا و سازمان‌های امنیتی در سازمان تشکیل می‌شود.

ج) مرکز مدیریت و هماهنگی عملیاتی زیرساخت‌ها : این مرکز به منظور ایجاد هم‌گرایی، هم‌افزایی، هماهنگی و هدایت عملیاتی بین زیرساخت‌های بااهمیت بالای کشور در شرایط عادی و عملیات پدافندی (اضطراری) با ماموریت‌های زیر تشکیل می‌گردد و با دریافت اطلاعات از وضعیت موجود زیرساخت و تحلیل آن به لحاظ آسیب‌پذیری و تهدیدات و اشتراک‌گذاری و تبادل اطلاعات مرتبط با آنها اقدام می‌کند:

1-Cyber Emergency Response Plan 2- Cyber Vulnerability Reduction Plan 3- Cyber Business Countinuty Plan 4- Cyber Disaster Recovery Plan
5- Cyber Critical Infrastructure Protection Plan 6- Cyber Preparedness Promotly Plan

۱) رصد و پایش وضعیت زیرساخت‌ها از منظر تهدیدات، آسیب‌پذیری و آمادگی،
۲) راهبری، مدیریت و ارائه برنامه کاهش دائمی آسیب‌پذیری مشترک زیرساختی،
۳) بهینه‌سازی و مدیریت وابستگی متقابل بین زیرساختی،
۴) رفع تعارض و ایجاد هماهنگی و هم‌افزایی 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) برنامه‌ریزی هماهنگ و مشترک در جهت پاسخ هم‌گرا به حوادث و تهدیدات،

ماده ۱۰– وظایف دستگاه‌های اجرایی

الف) وزارت راه و شهرسازی

۱) ملاحظات، الزامات، اصول و راهبردهای این طرح را در تهیه، بررسی و تصویب طرح‌های توسعه و عمران و طرح‌های‌کالبدی کشور اعمال و از اجرای آن اطمینان حاصل نموده و نتایج آن را هر ۶ماه به سازمان گزارش کند.
۲) ملاحظات، الزامات، اصول و راهبردهای این طرح را در کلیه سطوح خدمات مهندسی اعم از مطالعه، طراحی، اجرا و نظارت، اعمال و پیاده‌سازی کند.
۳) توانمندسازی آموزشی و تخصّصی ظرفیت‌های فنی و مهندسی (حقیقی و حقوقی) متناسب با نیاز این طرح را با استفاده از ظرفیت‌های موجود در سازمان نظام مهندسی و کنترل ساختمان، اجرا کند.
۴) اجرای این طرح را با هماهنگی سازمان در قالب اصول و قواعد فنی لازم‌الرعایه حفاظت از زیرساخت‌ها در ضوابط و مقرّرات ملی ساختمان، پیاده‌سازی، توسعه و ترویج نماید.
۵) ضوابط و راهکارهای کاهش خطرپذیری و بهینه‌سازی استحکام ساختمان‌ها 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 طرح‌های توسعه و عمران بنادر، فرودگاه‌ها، خطوط مواصلاتی شهری و بین شهری (ریلی، جاده‌ای، هوایی و دریایی) و خطوط ارتباطی بااهمیت 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 زیرساخت‌های بااهمیت‌بالا را با استفاده از ظرفیّت‌های موجود در دانشگاه صنعتی مالک اشتر با راهبری و هدایت سازمان تشکیل و راه‌اندازی کند.
۲) استانداردهای تخصّصی حفاظت از زیرساخت‌های 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 زیرساخت‌ها و سایر رشته -گرایش‌های مرتبط بین‌رشته‌ای با هماهنگی سازمان اقدام کند.
۴) نسبت به پژوهش و تولید و مدیریت دانش تخصّصی حفاظت از زیرساخت‌ها و بومی‌سازی آن در نظام آموزشی ذی‌ربط اقدام کند.
۵) نسبت به پشتیبانی از زیرساخت‌های 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 طرح‌های 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 طرح‌های 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 طرح‌های جامع حمل‌ونقل 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 پیاده‌سازی اهداف و ماموریت‌های این طرح به عمل آورد.

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

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

د)وزارت ارتباطات و فناوری اطلاعات

۱) نسبت به افزایش تاب‌آوری، 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 نرم‌افزارهای پرکاربرد، سیستم‌عامل‌ها، ایجاد و به روز نگه داشتن مخازن[1] نرم‌افزارها، مجوزهای[2] نرم‌افزاری پرکاربرد، سامانه‌های نام دامنه[3]، درجهت کاهش وابستگی کشور و بی‌اثرسازی اقدامات خصمانه دشمن در فضای سایبری اقدام کند.

۳) نسبت به ارتقای پایداری خدمات پدافند و امنیت سایبری مانند توانمندسازی افراد، ایجاد، سازماندهی و عملیاتی کردن تیم‌های واکنش به رخدادهای سایبری-CERT[4]- مدیریت وصله‌زنی[5] امنیتی، مقابله و کاهش حملات منع سرویس توزیع شده اقدام کند.

۴) نسبت به ایجاد شبکه‌های اختصاصی و محدود، آمن و مطمئن برای ارتباط زیرساخت‌های بااهمیت بالا با رعایت اصول پدافند و امنیت سایبری اقدام کند.

۵) ملاحظات، الزامات، اصول و راهبردهای این طرح را در تهیه، بررسی و تصویب طرح‌های 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 زیرساخت‌های با اهمیت بالا را در پروژه شبکه ملی اطلاعات پیاده‌سازی و اجرا کند.

هـ) وزارت علوم، تحقیقات و فناوری

۱) نسبت به طراحی رشته تحصیلی حفاظت از زیرساخت و برنامه‌ریزی جامع برای آموزش و تربیت نیروی انسانی متخصص در مقاطع کارشناسی،کارشناسی‌ارشد و دکتری در حوزه حفاظت از زیرساخت و سایر رشته -گرایش‌های مرتبط بین‌رشته‌ای با همکاری سازمان، اقدام کند.

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

۳) با هدایت توانمندی‌های مراکز رشد، شرکت‌های دانش‌بنیان، پارک‌های علم و فناوری تابعه و راه‌اندازی انجمن‌های علمی حفاظت از زیرساخت در دانشگاه‌های منتخب، نسبت به مطالعه، تدوین، تنظیم و به‌روزرسانی ضوابط، مقرّرات فنی- تخصصی حفاظت از زیرساخت در حوزه‌های کالبدی و سایبری اقدام کند.

1- Repository 2- Licence 3- DNS 4- Computer Emergency Response Team 5- Patch management

۴) با استفاده از ظرفیت دانشگاه‌ها، مراکز پژوهشی و پارک‌های علم و فناوری نسبت به پژوهش و تولید و مدیریت دانش تخصّصی حفاظت از زیرساخت‌ها و بومی‌سازی آن در نظام آموزش عالی اقدام کند.

۵) راهبردهای این طرح را در زیرساخت‌های با اهمیت بالای خود از قبیل آزمایشگاه‌های مرجع، دانشگاه‌ها و پژوهشگاه‌های تخصصی، پارک‌های علم و فناوری و مانند آن پیاده‌سازی و اجرا کند.

و) سازمان برنامه و بودجه کشور

۱) الزامات، ملاحظات و مقررات فنی و اجرایی مصوب کارگروه تنظیم مقررات حفاظت از زیرساخت‌های با اهمیت بالا را در برنامه‌ها، طرح‌ها و پروژه‌های حیاتی، حساس و مهم کشور نهادینه‌سازی کرده و اجرای آنها را از طریق کمیسیون مصوبات طرح‌های 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 طرح‌ها و پروژه‌های حیاتی، حساس و مهم حوزه‌های 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 - تحویل موقت و دائمی طرح و صدور پایان‌کار - پیش‌بینی نماید.

۳) در تدوین و تصویب برنامه ملی، بخشی، منطقه‌ای و استانی آمایش سرزمین و تصویب طرح‌های توسعه عمران و کالبدی کشور، ملاحظات راهبردی این طرح شامل کاهش مستمر آسیب‌پذیری‌ها، ارتقاء تاب‌آوری ملی، کاهش و بهینه‌سازی وابستگی متقابل راهبردی بین دستگاهی و تضمین تداوم کارکردهای اساسی کشور رعایت شود.

۴) چنانچه طرحی پس از اخذ مصوبه کمیسیون طرح‌های 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–دانشگاه جامع امام حسین (ع)

۱) مرکز تدوین، تنظیم و به روزرسانی ضوابط، مقررات فنی مهندسی حفاظت سایبری از زیرساخت‌های 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 راه‌اندازی کند.

۲) نسبت به آموزش و تربیت نیروی انسانی متخصّص در مقاطع کارشناسی، کارشناسی ارشد و دکتری در حوزه حفاظت از زیرساخت‌ها و سایر رشته –گرایش‌های مرتبط بین‌رشته‌ای اقدام کند.

۳) نسبت به پژوهش و تولید و مدیریت دانش تخصصی حفاظت از زیرساخت‌ها و بومی‌سازی آن در نظام آموزشی ذی‌ربط اقدام کند.

ح) وزارت اطلاعات و سازمان اطلاعات سپاه

۱) نسبت به مدیریت و کاهش تهدیدات درون‌زا در دستگاه‌های اجرایی اقدام و از آسیب‌ناپذیری یا حداقل آسیب‌پذیری ممکن اطلاعاتی و ضد اطلاعاتی زیرساخت‌های با اهمیت بالا اطمینان حاصل نماید.

۲) نسبت به رصد، پایش، تشخیص، برآورد و هشدار تهدیدات و آسیب‌پذیری‌ها و مخاطرات زیرساختی و اشتراک اطلاعاتی بین ذی‌نفعان اقدام کند.

۳) ضمن تامین، برآورد و اشراف اطلاعاتی مربوط به تهدیدات زیرساخت‌های با اهمیت بالا، در اجرای عملیات پدافند غیرعامل زیرساختی، پشتیبانی اطلاعاتی لازم از سازمان به‌عمل آورند.

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

ط) سازمان مناطق آزاد تجاری- صنعتی و مناطق ویژه اقتصادی کشور موظف است الزامات و ملاحظات این طرح و دستورالعمل‌های مربوط به آن را در طرح‌های جامع و کالبدی خود اعم از طرح‌های جدید و زیرساخت‌های موجود در مراحل مختلف (طراحی، ساخت و اجرا، بهره‌برداری) رعایت نموده و آخرین وضعیت پیاده‌سازی 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 زیرساخت‌های با اهمیت بالا و شریان‌های حیاتی مانند بنادر، فرودگاه‌ها، خطوط راه آهن و مانند آن، ظرف مدت یک‌سال، تدوین و تصویب کند.

۲) نظام فنی- تخصصی حفاظت از زیرساخت‌های کشور را پس از ۶ ماه از تاریخ ابلاغ این طرح، تهیه و ابلاغ کند.

۳) دستورالعمل حفاظت از زیرساخت‌های وابسته به سایبری را در برابر تهدیدات سایبری و الکترونیک و الکترومغناطیس را با مشارکت و همکاری دستگاه‌های اجرایی ذی‌ربط ظرف مدت یک‌سال، تهیه و ابلاغ کند.

۴) به‌منظور حصول اطمینان از اِعمال الزامات و مقرّرات پدافند غیرعامل در طرح‌های زیرساختی کشور نظام نظارت، کنترل فنی و صدور پایان‌کار پدافند غیرعامل طرح‌ها و پروژه‌های جدید و با اهمیت بالای کشور را تهیه و ابلاغ نموده و نتیجه اجرای آن را هر ۶ ماه به کمیته دائمی گزارش کند.

۵) به منظور حصول اطمینان از آمادگی زیرساخت‌های با اهمیت بالا در برابر تهدیدات مفروض، اجرای رزمایش‌های پدافند کالبدی و سایبری در مراکز حیاتی، حساس و مهم را به طور نوبه‌ای ارزیابی و کنترل نماید.

ماده ۱۱- اقدامات مشترک دستگاه‌های اجرایی

کلیه دستگاه‌های اجرایی مشمول، موظّف به اجرای موارد زیر می‌باشند:

۱) بازنگری و بازمهندسی نظام سطح‌بندی براساس مولفه‌های تعیین شده با قابلیت به روزرسانی دوره‌ای و اخذ تأییدیه از سازمان،

۲) تدوین، طراحی و پیاده‌سازی نظام عملیاتی روزآمد تداوم کارکرد و بازیابی در قالب زیرساخت‌ها و شریان‌های منعطف، مقاوم و تاب آور در برابر تهدیدات و حوادث،

۳) تهیه، بازنگری، به‌روز رسانی و پیاده‌سازی طرح‌های عملیاتی حفاظت فیزیکی و سایبری از زیرساخت‌های حیاتی، حساس و مهم خود اعم از:

۱- طرح پاسخ اضطراری به حوادث و تهدیدات زیرساختی، ۲- طرح تضمین و تسهیل تداوم کارکردهای اساسی،
۳- طرح بازیابی و برگشت‌پذیری زیرساختی، ۴- طرح اَمن‌سازی و مصون‌سازی زیرساختی،
۵- طرح کاهش آسیب‌پذیری‌های زیرساختی، ۶- طرح ارزیابی و ارتقاء آمادگی‌های زیرساختی،
۷- طرح بهینه‌سازی وابستگی و وابستگی‌های متقابل زیرساختی،

۴) ذخیره‌سازی، موازی‌سازی، اَمن‌سازی، جایگزینی خدمات، تطبیق‌پذیری با تمرکز بر برطرف نمودن یا موازی نمودن گره‌های زنجیره تولیدات و خدمات زیرساخت‌ها،

۵) ایجاد سامانه یکپارچه برای رصد، پایش، ارزیابی، تشخیص و هشداردهی روزآمد تهدیدات و آسیب‌پذیری‌ها در زیرساخت‌ها و شریان‌های حیاتی،

۶) تدوین و پیاده‌سازی برنامه عملیاتی مدیریت و کاهش تهدیدات درون‌زا در زیرساخت‌های با اهمیت بالا،

۷) تهیه، تدوین، اجرا و پیاده‌سازی نظام عملیاتی مصون‌سازی سایبری در زیرساخت‌های بااهمیت سایبری و وابسته به سایبر،

۸) اجرای برنامه‌های آموزشی منسجم و رزمایش هدفمند ارتقاء آمادگی و توانمندسازی مدیران و کارشناسان فعال در مراکز و زیرساخت‌های حیاتی، حساس و مهم متناسب با طرح‌های عملیاتی پدافندی زیرساختی،

۹) پیاده‌سازی رویکرد انتقال اقدامات و برنامه‌های پدافند غیرعاملی حفاظت از زیرساخت از پیوست به ذات طرح‌های توسعه زیرساختی در مراحل مطالعه و طراحی،

۱۰) تدوین و نهادینه‌سازی برنامه‌های مصون‌سازی تخصصی و مدیریت مخاطرات در زیرساخت‌های پرخطر،

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

۱۲) تهیه و تدوین طرح حفاظت از زیرساخت مراکز حیاتی، حساس و مهم خود-SSP[1]- ظرف یک‌سال از ابلاغ این طرح،

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

ماده ۱۲- استانداردها، الزامات و ملاحظات عمومی و تخصّصی پدافند غیرعامل حفاظت از زیرساخت‌های موجود و جدید حوزه‌های با اهمیت بالای کشور توسط سازمان تهیه، تنظیم و ابلاغ می‌شود و برای دستگاه‌های اجرایی و بخش‌خصوصی، لازم الاجراست.

ماده ۱۳- به منظور حصول اطمینان از رعایت الزامات و ملاحظات پدافند غیرعامل در اجرای طرح‌های عمرانی و زیرساخت‌های جدید (حیاتی، حساس و مهم) دستگاه‌های اجرایی موظّف به انجام آزمون پایداری طرح در برابر تهدیدات براساس طرح پایه، صحت‌سنجی اجرای طرح حفاظت از زیرساخت و اخذ تائیدیه پدافند غیرعامل از سازمان، جهت صدور پایانِ‌کار می‌باشند.

ماده ۱۴- حفاظت از اطلاعات و اسناد پدافند غیرعامل زیرساخت‌های با اهمیت بالا در اشکال مختلف آن از قبیل سند کتبی و پوشه الکترونیکی چند رسانه‌ای 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.

ماده ۱۵- اعتبار موردنیاز برای اجرای این طرح در زیرساخت‌های جدید براساس سازوکار پیش‌بینی 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، تامین می‌شود و اعتبار موردنیاز برای زیرساخت‌های درحال بهره‌برداری، براساس مطالعات و برآوردهای انجام شده توسط دستگاه اجرایی، در اعتبارات سالانه دستگاه، پیش‌بینی و تامین می‌گردد؛ بخش خصوصی و شرکت‌های غیردولتی دارای زیرساخت‌های با اهمیت‌بالا ملزم به تامین اعتبار موردنیاز اجرای طرح حفاظت از زیرساخت خود از منابع داخلی می‌باشند.

ماده ۱۶- سازمان با همکاری دستگاه‌های اجرایی ذی‌ربط، دستورالعمل‌ها و طرح‌های اجرایی موردنیاز برای پیاده‌سازی این طرح را تهیه و به دستگاه‌های اجرایی ابلاغ می‌کند.

ماده ۱۷- دستگاه‌های اجرایی موظفند هرگونه قصور و کوتاهی در اجرای این طرح در زیرساخت‌های حوزه‌های با اهمیت بالا را به سازمان گزارش کرده و برابر مقررات با فرد متخلّف، برخورد کنند.

ماده ۱۸- سازمان با مستنکفین از این طرح بنابر تخلّف صورت‌گرفته و براساس شیوه‌نامه‌ای که توسط سازمان تنظیم و ابلاغ می‌گردد برخورد انضباطی کرده و درصورت‌نیاز از طریق قوه قضائیه اقدام می‌کند.

ماده ۱۹- سازمان بر حسن اجرای این طرح، نظارت و اجرای آن را بصورت سالانه به کمیته‌ی دائمی گزارش کند.

فرماندهی کل قوا
کمیته دائمی (شورای عالی) پدافند غیرعامل کشور
جمهوری اسلامی ایران

1- Sector Specific Plan

ماده ۲۰- طرح راهبردی حفاظت از زیرساخت‌های کشور در بیست ماده و دو تبصره در تاریخ بیست‌ونهم شهریورماه سال یکهزار و چهارصدویک هجری‌شمسی در شصت‌وششمین جلسه کمیته‌دائمی به‌تصویب رسید.

طرح راهبردی حفاظت از زیرساخت‌های کشور مشتمل بر **بیست ماده و دو تبصره** که در تاریخ ۲۹/ ۰۶/ ۱۴۰۱ در شصت‌وششمین جلسه کمیته دائمی(شورای‌عالی) پدافند غیرعامل کشور به‌تصویب رسید، به استناد تبصره یک ماده نه اساسنامه سازمان پدافند غیرعامل کشور مصوّب **مقام معظّم رهبری وفرماندهی کل قوا**(مدظله‌العالی) جهت اجرا ابلاغ می‌گردد./هـ

رئیس ستاد کل نیروهای مسلح و کمیته دائمی پدافند غیرعامل کشور
سرلشکر پاسدار محمد باقری

فرماندهی کل قوا
کمیته دائمی (شورای عالی) پدافند غیرعامل کشور
جمهوری اسلامی ایران

گیرندگان:

۱. سردار رئیس محترم دفتر فرماندهی معظم کل قوا جهت استحضار معظّم له.
۲. دفتر رئیس محترم جمهوری اسلامی ایران جهت استحضار.
۳. دفتر رئیس محترم قوه قضاییه جهت استحضار.
۴. دفتر رئیس محترم مجلس شورای اسلامی جهت استحضار.
۵. سردار فرمانده محترم قرارگاه مرکزی حضرت خاتم الانبیاء (ص) جهت استحضار.
۶. وزیر محترم امور خارجه - جناب آقای دکتر حسین امیرعبداللهیان.
۷. وزیر محترم آموزش و پرورش – جناب آقای دکتر یوسف نوری.
۸. وزیر محترم ارتباطات و فناوری اطّلاعات - جناب آقای دکتر عیسی زارع‌پور.
۹. وزیر محترم اطّلاعات – حجت‌الاسلام والمسلمین سید اسماعیل خطیب.
۱۰. وزیر محترم اقتصاد و دارایی - جناب آقای دکتر احسان خاندوزی.
۱۱. وزیر محترم بهداشت، درمان و آموزش پزشکی - جناب آقای دکتر بهرام عین‌الهی.
۱۲. سرپرست محترم وزارت تعاون، کار و رفاه اجتماعی - جناب آقای دکتر محمدهادی زاهدی وفا.
۱۳. وزیر محترم جهاد کشاورزی - جناب آقای دکتر سیدجواد ساداتی نژاد.
۱۴. وزیر محترم دادگستری– جناب آقای دکتر امیرحسین رحیمی.
۱۵. وزیر محترم راه و شهرسازی - جناب آقای مهندس رستم قاسمی.
۱۶. وزیر محترم وزارت صنعت و معدن و تجارت - جناب آقای دکتر سیدرضا فاطمی امین .
۱۷. وزیر محترم علوم، تحقیقات و فناوری- جناب آقای دکتر محمدعلی زلفی‌گل.
۱۸. وزیر محترم فرهنگ و ارشاد اسلامی - جناب آقای دکتر محمدمهدی اسماعیلی.
۱۹. وزیر محترم میراث فرهنگی و گردشگری- جناب آقای دکتر سیدعزت اله ضرغامی.
۲۰. وزیر محترم نفت - جناب آقای مهندس جواد اوجی.
۲۱. وزیر محترم نیرو- جناب آقای مهندس علی اکبر محرابیان.
۲۲. وزیر محترم ورزش و امور جوانان- جناب آقای دکتر سیدحمید سجادی هزاوه.
۲۳. امیر فرمانده محترم کلّ ارتش جمهوری اسلامی ایران جهت استحضار.
۲۴. سردار فرمانده محترم کلّ سپاه پاسداران انقلاب اسلامی جهت استحضار.
۲۵. سردار فرمانده محترم نیروی انتظامی جمهوری اسلامی ایران جهت استحضار.
۲۶. سردار رئیس محترم سازمان بسیج مستضعفین جهت استحضار.
۲۷. رئیس محترم سازمان صدا وسیمای جمهوری‌اسلامی‌ایران- جناب‌آقای‌دکتر پیمان جبلی.
۲۸. رئیس محترم سازمان انرژی اتمی ایران- جناب آقای مهندس محمد اسلامی.
۲۹. رئیس محترم سازمان محیط زیست کشور- جناب آقای علی سلاجقه.
۳۰. رئیس محترم کل بانک مرکزی جمهوری اسلامی ایران - جناب آقای دکتر علی صالح‌آبادی.
۳۱. رئیس محترم سازمان تبلیغات اسلامی- حجت‌الاسلام والمسلمین محمد قمی.
۳۲. دبیرخانه شورای‌عالی امنیت ملی ج.ا.ا
۳۳. دبیرخانه شورای‌عالی آمایش سرزمین
۳۴. دبیرخانه شورای‌عالی علوم، تحقیقات و فنآوری (عتف)
۳۵. دبیرخانه شورای‌عالی فضای مجازی
۳۶. دبیرخانه شورای‌عالی معماری و شهرسازی ایران
۳۷. دبیرخانه شورای‌عالی هماهنگی ترافیک شهرهای کشور