



تمام معظّم رهبری: من شعار "دولت و ملت، همی و هم زبانی" را انتخاب کردم و امیدوارم این شعار در عمل تحقق پیدا کند.

مدیران عامل محترم کلیه شرکت‌های آب منطقه‌ای، سازمان آب و برق خوزستان، شرکت توسعه منابع آب و نیروی ایران و شرکت توسعه منابع آب و خاک سیستان

موضوع: ابلاغ سند راهبردی پدافند سایبری کشور

با سلام و احترام،

به پیوست نامه شماره ۱۶۰/۱/۵۸۵ مورخ ۹۴/۳/۲۱ رئیس محترم ستاد کل نیروهای مسلح و کمیته دائمی پدافند غیرعامل کشور در خصوص تصویب نامه سند راهبردی پدافند سایبری کشور جهت اجرا ارسال می گردد.

مهدی دانشگر

مدیر کل دفتر مدیریت بحران و پدافند غیرعامل

رونوشت:

تصویب نامه

وزیر محترم کشور

وزیر محترم دفاع و پشتیبانی نیروهای مسلح

معاون محترم رئیس جمهور و رئیس سازمان مدیریت و برنامه ریزی کشور

رئیس محترم کمیسیون امنیت ملی و سیاست خارجی مجلس شورای اسلامی

سردار رئیس محترم ارکان و امور مسلح مشترک نیروهای مسلح

سردار رئیس محترم سازمان پدافند غیرعامل کشور

سلام علیکم

با استحضار به محرم و آل محمد و احترام؛ کمیته دائمی (شورای عالی) پدافند غیرعامل کشور در جلسه مورخ ۱۳۹۴/۲/۲۹ به استناد ماده (۸)

اساسنامه سازمان پدافند غیرعامل کشور مصوب مقام معظم رهبری و فرماندهی کل قوا (مذکور)، «سند راهبردی پدافند سایبری کشور» پیشنهادی

سازمان پدافند غیرعامل کشور، موضوع بند ۱ ماده ۹ اساسنامه مذکور را بررسی و به شرح زیر تصویب نمود:

سند راهبردی پدافند سایبری کشور

ماده ۱: تعاریف و اصطلاحات

۱) فضای سایبری: به شبکه‌های وابسته به یکدیگر از زیرساخت‌های فناوری اطلاعات، شبکه‌های ارتباطی، سامانه‌های رایانه‌ای، پردازنده‌های تعبیه شده (جا گذاری شده)، کنترل کننده‌های صنایع حیاتی، محیط مجازی اطلاعات و اثر متقابل بین این محیط و انسان به منظور تولید، پردازش، ذخیره سازی، مبادله، بازیابی و بهره‌برداری از اطلاعات گفته می‌شود که ممکن است در ارتباط مستقیم و مداوم با سامانه‌های فناوری اطلاعات و شبکه‌های ارتباطی اعم از شبکه اینترنت باشد و یا تنها قابلیت اتصال به محیط پیرامونی، در آن تعبیه شده باشد.

۲) سرمایه ملی سایبری: بخشی از دارایی‌های کشور اعم از زیرساخت‌ها، سامانه‌ها، تجهیزات، نرم افزارها، اطلاعات و حتی افراد که در فرآیند تولید، پردازش، ذخیره سازی، مبادله، بازیابی و بهره‌برداری از داده‌های دارای اهمیت حیاتی، حساس و مهم در فضای سایبری کشور نقش مستقیم و تعیین کننده داشته باشند، سرمایه ملی سایبری نامیده می‌شود.

۳) آسیب پذیری سایبری: به ضعف، نقص و عیب موجود در داخل یک سرمایه ملی سایبری، رویه‌های امنیتی یا کنترل‌های داخلی، یا بیادسازی آن سرمایه ملی سایبری، که قابلیت بهره‌برداری یا فعال شدن تهدیدات داخلی و خارجی به منظور تهاجم و یا جنگ سایبری را داشت باشد، اطلاق می‌گردد.

۲۴۴۹۵
۹۴-۳-۲۵



تصویب نامه

وزیر محترم کشور

وزیر محترم دفاع و پشتیبانی نیروهای مسلح

معاون محترم رئیس جمهور و رئیس سازمان مدیریت و برنامه ریزی کشور

رئیس محترم کمیسیون امنیت ملی و سیاست خارجی مجلس شورای اسلامی

سردار رئیس محترم ارکان و امور مسلح مشترک نیروهای مسلح

سردار رئیس محترم سازمان پدافند غیرعامل کشور

سلام علیکم

باصولت بر محمد و آل محمد و احترام؛ کمیته دائمی (شورای عالی) پدافند غیرعامل کشور در جلسه مورخ ۲۹/۲/۱۳۹۴ به استناد ماده (۸)

اساسنامه سازمان پدافند غیرعامل کشور مصوب تمام معظم رهبری و فرماندهی کل قوا (مطالعاتی)، «سند راهبردی پدافند سایبری کشور» پیشنهادی

سازمان پدافند غیرعامل کشور، موضوع بند ۱ ماده ۹ اساسنامه مذکور را بررسی و به شرح زیر تصویب نمود:

سند راهبردی پدافند سایبری کشور

ماده ۱: تعاریف و اصطلاحات

۱) فضای سایبری: به شبکه‌های وابسته به یکدیگر از زیرساخت‌های فناوری اطلاعات، شبکه‌های ارتباطی، سامانه‌های رایانه‌ای، پردازنده‌های تعبیه شده (جا گذاری شده)، کنترل کننده‌های صنایع حیاتی، محیط مجازی اطلاعات و اثر متقابل بین این محیط و انسان به منظور تولید، پردازش، ذخیره سازی، مبادله، بازیابی و بهره‌برداری از اطلاعات گفته می‌شود که ممکن است در ارتباط مستقیم و مداوم با سامانه‌های فناوری اطلاعات و شبکه‌های ارتباطی اعم از شبکه اینترنت باشد و یا تنها قابلیت اتصال به محیط پیرامونی، در آن تعبیه شده باشد.

۲) سرمایه ملی سایبری: بخشی از دارایی‌های کشور اعم از زیرساخت‌ها، سامانه‌ها، تجهیزات، نرم افزارها، اطلاعات و حتی افراد که در فرآیند تولید، پردازش، ذخیره سازی، مبادله، بازیابی و بهره‌برداری از داده‌های دارای اهمیت حیاتی، حساس و مهم در فضای سایبری کشور نقش مستقیم و تعیین کننده داشته باشند، سرمایه ملی سایبری نامیده می‌شود.

۳) آسیب پذیری سایبری: به ضعف، نقص و عیب موجود در داخل یک سرمایه ملی سایبری، رویه‌های امنیتی یا کنترل‌های داخلی، یا پیاده‌سازی آن سرمایه ملی سایبری، که قابلیت بهره‌برداری یا فعال شدن تهدیدات داخلی و خارجی به منظور تهاجم و یا جنگ سایبری را داشته باشد، اطلاق می‌گردد.

۲۴۴۹۵

۹۴_۳_۲۵

۴) تهدید سایبری: احتمال هر گونه رویدادی که قابلیت وارد نمودن ضربه به مأموریت‌ها، وظایف، تصویر (بنداره) یا اشتهار دستگاه متولی سرمایه ملی سایبری یا افراد مرتبط، به واسطه یک سامانه اطلاعاتی، از طریق دسترسی غیرمجاز، انهدام (تخریب)، افشاء، تغییر اطلاعات و ایجاد اختلال یا ممانعت از ارائه خدمات را داشته باشد تهدید سایبری گفته می‌شود.

۵) تهاجم سایبری: به هرگونه اقدام غیرمجاز سایبری، که با هدف نقض سیاست امنیتی یک سرمایه سایبری و ایجاد خرابی یا خسارت، ایجاد اختلال در عملکرد یا از کار اندازی خدمات و یا دستیابی به اطلاعات انجام گیرد تهاجم سایبری گویند.

۶) جنگ سایبری: بالاترین سطح و پیچیده ترین نوع از تهاجم سایبری که توسط ارتش سایبری کشورهای مهاجم با گروه‌های سازماندهی شده تحت حمایت دولت‌های متخاصم علیه منافع ملی کشورها انجام می‌شود جنگ سایبری است.

۷) زیست بوم سایبری: به محیط بومی مشکل از زیرساخت‌های فناوری اطلاعات، شبکه‌های ارتباطی، سامانه‌های رایانه‌ای که به صورت زنده و پویا با عوامل انسانی در تعامل می‌باشد زیست بوم سایبری گفته می‌شود.

۸) سامانه‌های پایه سایبری: مجموعه‌ای از سخت افزارها و نرم افزارهایی که در شکل‌گیری فضای سایبری نقش اساسی داشته و مبنای طراحی و اجرای سایر سامانه‌ها می‌باشند سامانه‌های پایه سایبری است.

۹) دیپلماسی پدافند سایبری: به دفاع حقوقی از منافع ملی، تعامل و تبادل اطلاعات در قالب پیمان‌های مشترک سایبری بین کشورها دیپلماسی پدافند سایبری گفته می‌شود.

۱۰) پدافند سایبری: مجموعه اقدامات سایبری و غیر سایبری است که توانمندی رصد، پایش، تشخیص تهدید، استخراج آسیب پذیری، تجزیه و تحلیل میزان خطر، مدیریت و کنترل تهاجم سایبری، بازیابی اطلاعات و تولید قدرت پاسخگویی به تهدید سایبری دشمن را ایجاد کند و موجب مصون‌سازی، کاهش آسیب‌پذیری و حفاظت از سرمایه‌های ملی سایبری و زیست بوم سایبری کشور شود و با تولید بازدارندگی امکان تهاجم سایبری را از کلیه متخاصمین سلب نماید.

۱۱) نظام جامع بومی پدافند سایبری: نظامی است بومی، مشکل از زیر نظام‌های رصد، پایش، تشخیص، مدیریت و کنترل بهنگام، تولید و کنترل آمادگی، مدیریت بحران، دفاع حقوقی، منابع انسانی (آموزش، نیروی انسانی، مدیریت، مهارت، ساختار)، آموزش و فرهنگ‌سازی، صنعت سایبری، هشدار و اطلاع‌رسانی، حفاظت و امنیت در حوزه پدافند سایبری که برای انجام مأموریت‌های پدافند سایبری کشور ایجاد می‌شود.

ماده ۲: چشم انداز پدافند سایبری کشور

با یاری خداوند قادر متعال، جمهوری اسلامی ایران در آفت ۱۴۰۴، کشوری است؛ دست یافته به زیست بوم ملی سایبری امن، مصون، پایدار در برابر تهدیدات و حملات سایبری دشمن و قدرت برتر پدافند سایبری و دارای جایگاهی ممتاز در بین کشورهای منطقه و



بوخوردار از:

- ۱) نظام جامع بومی پدافند سایبری هوشمند، پایدار و مقاوم، انحصاری، ابتکاری، لایه به لایه، شبکه ای، چابک و منعطف در سطوح ملی، دستگاهی و استانی
- ۲) نظام مدیریت و کنترل جامع و هوشمند با قابلیت رصد، پایش، تشخیص، هشدار و مدیریت و کنترل بهنگام صحنه عملیات پدافند سایبری
- ۳) مصوبیت در زیرساخت های حیاتی، استحکام و پایداری در زیر ساخت های حساس و امنیت و ایمنی در زیر ساخت های مهم
- ۴) سرمایه های انسانی مؤمن، متعهد مجرب، آموزش دیده و متخصص در حوزه پدافند سایبری و دارای تفکر بسیجی و روحه جهادی
- ۵) نظام دیپلماسی پدافند سایبری فعال، متعامل، مشارکت جو و مدافع منافع ملی سایبری
- ۶) صنعت بومی پدافند سایبری روزآمد، رقابتی و پاسخ گو به تهدید، خود اتکا و اقتصادی در تولید سامانه های پایه پدافند سایبری با بهره گیری از ظرفیت های کشور
- ۷) استانداردها و الگوهای پدافند سایبری بومی، امن، پویا و روزآمد
- ۸) جایگاه ممتاز علمی و فناوریانه در حوزه پدافند سایبری منطقه
- ۹) توانمندی مدیریت بحران سایبری در راستای تداوم خدمات رسانی ضروری
- ۱۰) نظام نهادینه شده آموزش و فرهنگ سازی پدافند سایبری در متن فرهنگ عمومی و نظام آموزشی کشور
- ۱۱) مشارکت ظرفیت بخش های دولتی، غیردولتی، مردم نهاد و بسیج در پدافند سایبری
- ۱۲) نظام تولید، حفظ و ارتقاء آمادگی های پدافند سایبری در برابر تهدیدات

ماده ۳: ارزش های اساسی حاکم بر حوزه پدافند سایبری کشور

- ۱) خودباوری و خودانکابی
- ۲) اعتماد سازی، اطمینان بخشی
- ۳) نوآوری و خلاقیت
- ۴) اخلاق اسلامی
- ۵) نفی سلطه دشمن
- ۶) فرهنگ و ارزش های اسلامی
- ۷) مدیریت جهادی
- ۸) تفکر و عمل بسیجی



ماده ۴: اصول حاکم بر حوزه پدافند سایبری کشور

- ۱- مصون سازی و پایداری
- ۲- وحدت مدیریت
- ۳- بازدارندگی
- ۴- حفظ آمادگی
- ۵- پیش بینی در تهدیدشناسی
- ۶- اقتصادی سازی (رعایت صرفه و صلاح)
- ۷- اشراف اطلاعاتی
- ۸- دیپلماسی فعال
- ۹- اقتدار درون زا

ماده ۵: رسالت پدافند سایبری کشور

"پدافند سایبری از سرمایه های ملی، سایبری و فضای سایبری کشور در برابر تهدیدات و حملات سایبری دشمن"

قرارگاه پدافند سایبری کشور رسالت مصون سازی و پایداری سازی سامانه های سایبری کشور از طریق رصد، پایش و تشخیص تهدیدات، کشف، مدیریت و کنترل آسیب پذیری ها، اعلام هشدارهای لازم، اطمینان از پدافند سایبری، تدوین و انتشار نظامات (ملاحظات، مقررات، الزامات و اصول) پدافندی، آموزش و نهادینه سازی پدافند سایبری، مدیریت عملیات پدافند سایبری و دفاع حقوقی در برابر تهدیدات و حملات دشمن را بر عهده دارد.

ماده ۶: مأموریت های عمده قرارگاه پدافند سایبری کشور

- ۱) هدایت، راهبری، نظارت و هماهنگی فرماندهی عملیاتی پدافند سایبری از زیرساخت های اساسی کشور متناسب با سطح اهمیت آنها (مصون سازی زیرساخت های حیاتی سایبری، مستحکم و پایداری سازی زیرساخت های حساس سایبری و ایمن سازی و کاهش آسیب پذیری زیرساخت های مهم سایبری کشور)
- ۲) رصد، پایش و تشخیص تهدیدات سایبری دشمن و هشدار و تعیین وضعیت آن
- ۳) هدایت و راهبری ایجاد توانمندی ها و ظرفیت های احتیاط راهبردی برتر ساز در حوزه پدافند سایبری
- ۴) هدایت و راهبری پدافند سایبری هوشمند، چند لایه و اثربخش از سرمایه های سایبری کشور
- ۵) هدایت و راهبری کنترل عملیاتی پدافند سایبری در سطوح ملی، منطقه ای و دستگاہی
- ۶) هدایت و راهبری ایجاد و ارتقاء نظام جامع پدافند سایبری کشور



- ۷) هدایت و راهبری ایجاد و ارتقاء آمادگی پدافند سایبری در دستگاه‌های اجرایی ملی و استانی، بخش غیردولتی و اتحاد جامعه
- ۸) هدایت و راهبری مصون سازی، پایدارسازی و استحکام زیست بوم سایبری و سرمایه‌های ملی سایبری کشور
- ۹) نظارت و حصول اطمینان از تولید و بکارگیری سامانه‌های پایه و اساسی پدافند سایبری کشور
- ۱۰) هدایت و راهبری جلب مشارکت ظرفیت‌های بخش‌های دولتی، غیردولتی، مردم و بویژه بسیج در پدافند سایبری
- ۱۱) هدایت و راهبری ایجاد و ارتقاء ظرفیت‌های صنعت بومی دفاع سایبری کشور (دولتی و غیردولتی)
- ۱۲) نهادینه سازی اصول، الزامات و ملاحظات فنی پدافند سایبری در متن برنامه‌ها و طرح‌های توسعه سایبری کشور
- ۱۳) هدایت و راهبری توسعه و پایدارسازی معماری پدافند سایبری در زیرساخت‌های دارای اهمیت
- ۱۴) نهادینه سازی آموزه‌های پدافند سایبری در متن برنامه‌های آموزشی و فرهنگ سازی کشور در سطوح مختلف
- ۱۵) هدایت و راهبری ایجاد و ارتقاء نظام اطلاع رسانی و عملیات روانی در فضای سایبری در برابر دشمن
- ۱۶) هدایت و راهبری آموزش‌های تخصصی تربیت نیروی انسانی متخصص در حوزه پدافند سایبری
- ۱۷) هدایت و راهبری تولید و مدیریت دانش در حوزه پدافند سایبری
- ۱۸) هدایت و راهبری دیپلماسی پدافند سایبری

توضیح: قرارگاه پدافند سایبری مسئولیت هر یک از دستگاه‌های اجرایی کشور مرتبط با اجرای مأموریت‌های مندرج در این ماده را حد اکثر یک سال پس از ابلاغ سند با مشارکت و هماهنگی دستگاه مربوط تهیه و جهت تصویب به دبیرخانه کمیته دائمی ارائه نماید.

ماده ۷: اهداف کلان در افق چشم انداز پدافند سایبری کشور

- ۱) دستیابی به نظام جامع بومی پدافند سایبری
- ۲) دستیابی به زیرساخت‌ها و سرمایه‌های ملی مصون سایبری
- ۳) دستیابی به زیست بوم سایبری امن، مصون و پایدار
- ۴) دستیابی به منابع انسانی توانمند و کارآمد پدافند سایبری
- ۵) دستیابی به جایگاه ممتاز علمی و فناوری پدافند سایبری منطقه
- ۶) دستیابی به صنعت بومی خود اتکا و پیشرفته پدافند سایبری
- ۷) دستیابی به استانداردها و الگوهای پدافند سایبری بومی، امن، پویا و روزآمد
- ۸) دستیابی به دیپلماسی فعال پدافند سایبری

- ۹) دستیابی به ظرفیت مناسب فرماندهی و کنترل پدافند سایبری
- ۱۰) نهادینه سازی فرهنگ، ادبیات و آموزه‌های پدافند سایبری
- ۱۱) دستیابی به مشارکت ظرفیت‌های بخش‌های دولتی و غیردولتی در حوزه پدافند سایبری
- ۱۲) حفظ و ارتقاء آمادگی‌های پدافندی سایبری در برابر تهدیدات

ماده ۸: راهبردهای پدافند سایبری کشور

- ۱) طراحی، پیاده‌سازی و راهبری نظام جامع بومی پدافند سایبری هوشمند، پایدار و مقاوم، انحصاری، ابتکاری، لایه به لایه، پیش‌گیرانه، شبکه‌ای، چابک و منعطف در سطوح ملی، دستگاهی و استانی
- ۲) طراحی، پیاده‌سازی و راهبری طرح‌ها و برنامه‌های پدافند سایبری از زیرساخت‌های کشور برای مصون‌سازی زیست بوم سایبری در برابر تهدیدات و تهاجم سایبری متناسب با سطح اهمیت آنها.
- ۳) الزام و همراه سازی سازمان‌های متولی زیرساخت‌های حیاتی و حساس کشور در استفاده از محصولات سایبری امن بومی.
- ۴) بکارگیری منابع انسانی متخصص و امین یا ساماندهی و ارتقای کمی و کیفی در حوزه پدافند سایبری.
- ۵) تولید و مدیریت دانش و فناوری پدافند سایبری متناسب با تهدیدات.
- ۶) بومی و امن سازی سامانه‌های سایبری مورد استفاده در زیرساخت‌های حیاتی و حساس کشور با تاکید بر ممنوعیت کاربرد سامانه‌های خارجی در آنها (در جهت کاهش وابستگی به فناوری‌ها و محصولات غیر بومی).
- ۷) ساماندهی و تقویت صنعت پدافند سایبری بومی و حمایت از سازمان‌ها و شرکت‌های تولیدکننده دولتی و غیردولتی و محصولات بومی و روزآمد.
- ۸) سازماندهی، حمایت و صیانت از تولید امن داخلی سامانه‌های پایه و اساسی پدافند سایبری کشور.
- ۹) بومی سازی فرآیندها، نظام‌ها و استانداردها، پروتکل‌های فنی، رویه‌ها و روال‌های پدافند سایبری.
- ۱۰) طراحی، پیاده‌سازی و راهبری نظام دیپلماسی پدافند سایبری کشور.
- ۱۱) طراحی، پیاده‌سازی و راهبری سامانه فرماندهی و کنترل پدافند سایبری.
- ۱۲) فرهنگ سازی و آموزش تخصصی و عمومی مسئولین و نخبگان و آحاد جامعه در حوزه پدافند سایبری.
- ۱۳) نهادینه سازی آموزه‌های پدافند سایبری در نظام آموزشی (ابتدایی، متوسطه و دانشگاهی) و نظام آموزش دفاعی کشور.
- ۱۴) بهره‌گیری از قابلیت‌های سازمان بسیج مستضعفین و سازمان‌های مردم نهاد و ظرفیت‌های بخش غیردولتی در پدافند سایبری.
- ۱۵) مدیریت بر ارتقاء ضریب پایداری، مصون سازی، ارتقاء توان بازدارندگی زیرساخت‌های حیاتی و حساس کشور در برابر تهدیدات و حملات سایبری.



جمهوری اسلامی ایران

فرماندهی کل قوا
کمیته دائمی پدافند غیرعامل کشور

شماره: ۱۶۰/۱/۵۸۵
تاریخ: ۱۳۹۴/۰۳/۲۱
پیوست: ندارد

- ۱۶) حفاظت و تامین امنیت هوشمندانه سایبری از زیرساخت‌ها و طرح‌ها متناسب با سطح اهمیت آنها.
 - ۱۷) استفاده هوشمندانه (توجه به فرصت‌ها و تهدیدات فناوری‌ها) از سامانه‌های جدید سایبری در زیرساخت‌های دارای اهمیت.
 - ۱۸) مشارکت در تدوین راهبردها علیه تهدیدات مشترک نظامی و سایبری.
 - ۱۹) راهبری، هدایت، ایجاد هماهنگی و هم‌افزایی راهبرد محور پدافند سایبری در کلیه دستگاه‌های اجرایی.
 - ۲۰) طراحی و پیاده‌سازی و راهبری نظام جامع رصد، پایش، تشخیص و هشدار در مقابل تهدیدات سایبری دشمن.
- این سند که در هشت ماده و نود بند و یک تبصره در جلسه مورخ ۱۳۹۴/۰۲/۲۹ کمیته دائمی بررسی و به تصویب رسیده به استناد تبصره ۱ ماده ۹ اساسنامه سازمان پدافند غیرعامل کشور مصوب مقام معظم رهبری و فرماندهی کل قوا (مدعاه انساب) جهت اجرا ابلاغ می‌گردد.

رئیس ستاد کل نیروهای مسلح و کمیته پدافند غیرعامل کشور
سرلشکر سپهبد دکتر سید حسن فیروزآبادی



فهرست:

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 قضائیه جهت استحضار.
۴. دفتر رئیس محترم مجلس شورای اسلامی جهت استحضار.
۵. وزیر محترم امور خارجه - جناب آقای دکتر محمدجواد ظریف .
۶. وزیر محترم آموزش و پرورش - جناب آقای دکتر علی اصغر فانی .
۷. وزیر محترم ارتباطات و فناوری اطلاعات - جناب آقای دکتر محمود واعظی .
۸. وزیر محترم اطلاعات - حجت الاسلام والمسلمین سید محمود علوی .
۹. وزیر محترم اقتصاد و دارایی - جناب آقای دکتر علی طیب نیا .
۱۰. وزیر محترم بهداشت، درمان و آموزش پزشکی - جناب آقای دکتر سید حسن قاضی زاده هاشمی .
۱۱. وزیر محترم تعاون، کار و رفاه اجتماعی - جناب آقای دکتر علی ربیعی .
۱۲. وزیر محترم جهاد کشاورزی - جناب آقای مهندس محمود جنتی .
۱۳. وزیر محترم دادگستری - حجت الاسلام والمسلمین مصطفی پورمحمدی .
۱۴. وزیر محترم راه و شهرسازی - جناب آقای دکتر عباس آخوندی .
۱۵. وزیر محترم صنعت و معدن و تجارت - جناب آقای مهندس محمدرضا نعمت زاده .
۱۶. وزیر محترم علوم، تحقیقات و فناوری - جناب آقای دکتر محمد فرهادی .
۱۷. وزیر محترم فرهنگ و ارشاد اسلامی - جناب آقای دکتر علی جنتی .
۱۸. وزیر محترم نفت - جناب آقای مهندس بیژن نامدار زنگنه .
۱۹. وزیر محترم نیرو - جناب آقای مهندس حمید چیت چیان .
۲۰. امیر فرمانده محترم کل ارتش جمهوری اسلامی ایران جهت استحضار .
۲۱. سردار فرمانده محترم کل سپاه پاسداران انقلاب اسلامی جهت استحضار .
۲۲. سردار فرمانده محترم نیروی انتظامی جمهوری اسلامی ایران جهت استحضار .
۲۳. سردار رئیس محترم سازمان بسیج مستضعفین جهت استحضار .
۲۴. رئیس محترم سازمان انرژی اتمی ایران - جناب آقای دکتر علی اکبر صالحی جهت استحضار .
۲۵. رئیس کل محترم بانک مرکزی جمهوری اسلامی ایران - جناب آقای دکتر ولی الله سیف جهت استحضار .
۲۶. رئیس محترم سازمان تبلیغات اسلامی - حجت الاسلام والمسلمین سید مهدی خاموشی جهت استحضار .