	تشریح پروژه واگذاری	
	TDF02-0	
	CoRFP20-6	

عنوان پروژه:	**شناسایی دارایی‌های مبتنی بر ICT در نیروگاه نمونه و مدیریت مخاطرات امنیتی**
عنوان طرح:	**طرح توسعه زیرساخت‌های امنیتی در صنعت برق**
واحد اجرایی:	**مرکز توسعه فناوری امنیت اطلاعات، ارتباطات و تجهیزات صنعت برق**

برآورد کلی مدت زمان اجرای پروژه: ۶ ماه

تبیین و تشریح پروژه همراه با ذکر مراحل کلی:

از آنجا که نیروگاه‌ها به عنوان تولیدکنندگان نیروی برق، یکی از ارکان صنعت برق و از مهمترین زیرساخت‌های حیاتی کشور هستند، استفاده از آسیب‌پذیری‌های سایبری در سیستم‌های مبتنی بر ICT در بخش تولید و نیروگاه‌های کشور می‌تواند مشکلات متعددی از جمله کاهش میزان تولید برق، قطعی برق و ایجاد نارضایتی مشترکین را به دنبال داشته باشد لذا شناخت نقاط آسیب پذیر و رفع آنها و استفاده از روش‌های مقاوم‌سازی قبل از وقوع حملات امنیتی ضروری است.

هدف از این پروژه، بررسی وضعیت موجود، شناخت دارایی‌ها، تحلیل مخاطرات موجود در یک نیروگاه، پیشنهاد کنترل‌های امنیتی جهت ارتقاء امنیت هر یک از دارایی‌ها در یک نمونه از نیروگاه‌های مرتبط با شرکت مادر تخصصی تولید نیروی برق حرارتی است که می‌تواند از یکی از انواع گازی، بخاری و یا سیکل ترکیبی باشد.

در این پروژه دارایی‌ها در بخش کنترل صنعتی نیروگاه نمونه استخراج شده و ارزش هر دارایی تعیین و شناسایی آسیب‌پذیری‌های هر دارایی انجام می‌گیرد. تعیین تهدیدها، احتمال وقوع تهدیدها، نگاشت تهدیدها و آسیب‌پذیری‌ها و در نهایت محاسبه ریسک از جمله فعالیت‌هایی است که برای دارایی‌های مبتنی بر ICT نیروگاه نمونه باید انجام گیرد. تحلیل مخاطرات به عنوان سند این بخش برای نیروگاه نمونه باید تهیه گردد. تعیین الزامات امنیتی و کنترل‌های مرتبط با هر آسیب‌پذیری در ادامه انجام شده و سپس بر اساس ریسک و مخاطرات شناسایی شده، کنترل‌های امنیتی جهت اجرا، اولویت‌بندی می‌شوند و در نهایت سند مدیریت مخاطرات تهیه و ارائه می‌گردد. همچنین باید محاسبه گردد که در صورت پیاده‌سازی الزامات و کنترل‌های امنیتی، سطح امنیتی مورد نیاز با توجه به ریسک شناسایی شده، تا چه میزان ارتقاء می یابد. اگرچه بررسی و ممیزی دائم در بحث مدیریت مخاطرات از الزامات است، در این پروژه فقط فاز اولیه پیشنهاد و اولویت‌بندی کنترل‌های امنیتی در نظر گرفته شده و اجرا، پیاده‌سازی کنترل‌ها و پایش مجدد پس از اجرایی شدن پیشنهادات در پروژه دیگری انجام خواهد شد.

نکته : شرکت‌های پیشنهاددهنده باید دارای پروانه فعالیت در حوزه ارائه خدمات مدیریتی افتا از سازمان فناوری اطلاعات باشند و نام آن‌ها در سایت اداره کل نظام مدیریت امنیت اطلاعات (نما) قابل پیگیری باشد.

مشخصات محصول نهایی(خروجی مورد انتظار):

- ارائه لیست کلیه دارایی‌ها در زیرسیستم‌های صنعتی مبتنی بر ICT در نیروگاه نمونه و تعیین ارزش هر یک از دارایی‌ها
- ارائه گزارشی از آسیب‌پذیری‌ها و تهدیدات هر یک از دارایی‌های شناسایی شده
- ارائه گزارشی از تخمین احتمال هر رخداد سایبری مرتبط با دارایی‌های شناسایی شده و میزان خسارت احتمالی آن
- ارزیابی و تحلیل مخاطرات امنیتی بخش کنترل صنعتی نیروگاه و ارائه سند تحلیل مخاطرات امنیت سایبری مرتبط
- تهیه سند مدیریت مخاطرات در بخش کنترل صنعتی مبتنی بر ICT نیروگاه نمونه و ارائه کنترل‌های پیشنهادی در هر بخش از نیروگاه و بررسی تاثیر آن بر مخاطرات پیش‌بینی شده