Preguntas y respuestas sobre notificación de necesidad de servicios profesionales número PRITS 2023-0001

Para establecer contratos para la coordinación y desarrollo de un plan de ciberseguridad para el Gobierno de Puerto Rico

Contenido

1. Introducción

Con el fin de proporcionar claridad y responder a las preguntas e inquietudes de los posibles interesados en presentar propuestas, la Oficina del Puerto Rico Innovation and Technology Service (PRITS) ha desarrollado este documento de preguntas y respuestas (Q&A). A continuación, se presentan las preguntas recibidas junto con sus respectivas respuestas, las cuales han sido organizadas por categoría o tema relevante. El propósito de PRITS es utilizar esta herramienta para promover la transparencia y la equidad en el proceso, fomentando así una competencia justa y una comprensión clara de los requisitos y expectativas asociados a este proyecto de ciberseguridad.

2. Preguntas

A. Alcance

1. Esta solicitud, ¿es para la agencia PRITS en general? ¿Necesita PRITS una recomendación contemplando las demás agencias del gobierno en general?

   La solicitud de servicios profesionales y la posible posterior contratación será realizada por PRITS. No obstante, el plan deberá estar diseñado para la protección contra los riesgos y amenazas de ciberseguridad de los sistemas de información propiedad de y operados por, o en nombre del Gobierno de Puerto Rico y los municipios.

2. Se menciona Gobernanza en varios renglones. Como parte de la solicitud, ¿requieren se incluyan servicios de Data y/o IT Gobernanza?

   La notificación de necesidad de servicios profesionales tiene como objetivo primordial el establecimiento de estructuras de gobernanza que inician con la elaboración de un plan de ciberseguridad con el fin de fortalecer las capacidades de respuesta a incidentes de ciberseguridad y asegurar la continuidad de las operaciones gubernamentales.
   PRITS reconoce que hay una interconexión entre los sistemas de datos y otros sistemas de IT, pero los servicios solicitados en PRITS 2023-001 no abarcan servicios de datos ni la implementación de otras iniciativas de gobernanza para los sistemas de información.

3. ¿Favor de abundar sobre el alcance… se requiere la revisión de los procedimientos que actualmente tienen o la creación de un formato (*template*)?

   Los proponentes deberán considerar las políticas, los procedimientos estándar existentes y otros documentos de apoyo vigentes para identificar las fortalezas y áreas de mejora que se incluirán en el plan de ciberseguridad. Es importante que los proponentes evalúen la alineación de estos documentos con las mejores prácticas, el marco de ciberseguridad a ser desarrollado en el plan y las normativas estatales y federales aplicables.

4. ¿Se pretende que los "servicios" especificados en la parte superior de la página 20 sean servicios únicos que se propongan además del desarrollo del Plan Estratégico de Ciberseguridad, O se pretende que estos servicios estén incluidos y abordados en el Plan Estratégico de Ciberseguridad como "objetivos" del plan, etc.?

   Los servicios especificados en la página 20 deberán ser integrados como elementos del Plan Estratégico para reducir el riesgo de ciberseguridad y aumentar las capacidades a nivel gubernamental. Para más detalles sobre lo que debe contener el Plan, al final de este documento se incluye el Apéndice C del Aviso de Oportunidad de Financiamiento (NOFO, por sus siglas en inglés) del Departamento de Seguridad Nacional para el Programa de Subvenciones de Ciberseguridad Estatal y Local (SLCGP) del Año Fiscal 2022.

5. ¿Puede PRITS proporcionar detalles adicionales sobre el alcance de las políticas de parches que se actualizarán y mejorarán, y a qué tipos de sistemas operativos de servidores/estaciones de trabajo, aplicaciones, dispositivos de red, etc. se aplicarán las políticas de parches?

   Durante el proceso de desarrollo del plan, se espera que se proporcione esta información. No obstante, la misma no está contemplada en el alcance de este aviso.

6. ¿Puede PRITS proporcionar información adicional y aclaraciones sobre el "ejercicio de simulación de mesa" y el "ejercicio a gran escala", incluyendo las entidades gubernamentales y funcionarios involucrados y/o cualquier participante de los municipios, propietarios y operadores de infraestructura crítica, etc., que participarán, así como el alcance de las redes, sistemas y activos que se abordarán en los ejercicios de simulación de mesa y a gran escala?

   Se espera que los empleados, principalmente aquellos encargados de velar por infraestructura crítica, participen de un ejercicio de simulación de mesa donde se recreen escenarios hipotéticos de ataques cibernéticos o incidentes de seguridad con el fin de evaluar y mejorar la capacidad de respuesta de un equipo de IT o de una agencia frente a estas situaciones. Este tipo de ejercicio permitirá analizar roles y responsabilidades, evaluar las estrategias de respuesta, identificar brechas en los procedimientos y realizar mejoras para fortalecer la resiliencia y capacidad de respuesta ante futuros eventos.

   En el ejercicio a gran escala se espera una simulación que involucre múltiples agencias, entidades u otros participantes relevantes. A través de este ejercicio se espera evaluar la respuesta gubernamental frente a ciberataques de gran envergadura o incidentes de seguridad complejos. Bajo este tipo de escenario se espera poner a prueba la coordinación, comunicación, colaboración y las capacidades técnicas de las agencias participantes. Del mismo modo, este tipo de ejercicio podría utilizarse para identificar fortalezas, debilidades y áreas de mejora del plan, así como de otras herramientas o normativas, con el fin de mejorar la postura gubernamental en materia de ciberseguridad.

7. Se recomienda enumerar las agencias incluidas y excluidas en el Alcance del Trabajo (SOW).
    a. Según el directorio adjunto, hay 170 agencias/subagencias en PR hasta mayo de 2017.

Si bien el objetivo es que el plan abarque a todo el Gobierno de Puerto Rico y los municipios, esta fase inicial estará centrada en analizar la postura de ciberseguridad de agencias críticas, que incluyen las siguientes:

- *Departamento de Educación*
- *Departamento de la Familia*
- *Departamento de Salud*
- *Departamento de Seguridad Pública*
- *Departamento de Hacienda*

B. Campaña de *Phishing* y Campaña de Educación

1. ¿Puede PRITS proporcionar aclaraciones sobre el alcance de la campaña de phishing?

El plan estratégico de ciberseguridad debe contemplar la implementación de campañas de concienciación y educación sobre el phishing dirigidas a todos los empleados del Gobierno de Puerto Rico y de los municipios. Estas campañas tienen como objetivo proporcionar información clara y concisa sobre las tácticas de phishing, enseñar a identificar correos electrónicos sospechosos, ofrecer directrices sobre cómo actuar en caso de recibir uno y promover las mejores prácticas de seguridad en línea.

Además, se sugiere la inclusión de simulaciones de ataques de phishing para evaluar la susceptibilidad y respuesta de los empleados y proporcionar retroalimentación que contribuya a mejorar las prácticas de seguridad y sus habilidades de detección.

2. ¿Incluirá la educación masiva y la campaña de phishing al personal del Gobierno de Puerto Rico en general, a funcionarios de los municipios y/o los ciudadanos de Puerto Rico?

Las campañas de phishing a incluirse en el plan deben involucrar a todos los empleados del Gobierno de Puerto Rico y los municipios, sin importar su posición, nivel jerárquico o entidad gubernamental a la que pertenezcan.

Además, una vez que el Plan sea aprobado, se espera llevar a cabo una campaña masiva de educación en ciberseguridad y difusión del plan durante el mes de la ciberseguridad (octubre). Esta campaña se dirigirá a los empleados del Gobierno Central, los municipios y las entidades privadas que operan o administran sistemas de IT en nombre del Gobierno de Puerto Rico y los municipios.

3. ¿Cuál será la recurrencia de campaña?

En el contexto de esta notificación, se requiere que el plan contemple la implementación periódica y actualización de campañas de phishing. El propósito es fomentar una cultura de seguridad cibernética y concienciar sobre los riesgos del phishing, lo cual puede contribuir a prevenir ataques y proteger la información sensible del Gobierno de Puerto Rico y los municipios.

Por otra parte, según la solicitud de servicios, se espera llevar a cabo la campaña de educación masiva y difusión del plan estratégico de ciberseguridad en octubre de 2023.

C. Certificaciones/Credenciales

1. Existe un requerimiento de credenciales de EMAP y ANSI/EMAP; ¿es compulsorio que compañías que soliciten para subvenciones en esta propuesta que tengan estas credenciales al momento de solicitar?

   No se requiere que los proponentes presenten credenciales específicas de EMAP o ANSI. Sin embargo, se sugiere que los proponentes presenten certificaciones pertinentes al ámbito de la ciberseguridad y al tipo de servicio solicitado.

D. Contratación

1. ¿Cuál sería el término del contrato?

   Por regla general, los contratos con el Gobierno se llevan a cabo conforme año fiscal de julio a junio del siguiente año.

2. Aunque tenemos la capacidad operacional para ejecutar los servicios incluidos en el AVISO de forma autónoma, en algunos de los servicios listados tenemos socios de negocio que nos apoyan en cuanto a la tecnología y/o personal operacional para lograr el mayor costo beneficio de nuestros servicios manejados. ¿Está permitido subcontratar parcialmente los servicios? De ser permitido; ¿Cuál es el protocolo para declarar nuestros aliados?

   Por regla general los servicios contratados por PRITS no se puede subcontratar ni tampoco se pueden contratar peritos u otras personas sin el previo consentimiento escrito del PRITS. La solicitud para contratar a un tercero debe especificar los asuntos o casos en los que intervendrá el consultor y este deberá cumplir con cada uno de los requisitos de contratación con el Gobierno.

3. ¿Puede PRITS confirmar que un proponente o proponentes a los que se les adjudique un contrato para llevar a cabo cualquier servicio bajo esta notificación (es decir, "Proponente Afortunado") no se verá(n) impedido(s) de participar en ninguna otra solicitud de propuesta o proyectos derivados del desarrollo del Plan Estratégico de Ciberseguridad u otros servicios realizados de acuerdo con esta notificación?

Los "proponentes afortunados" podrían participar en otras solicitudes siempre y cuando las mismas no estén en contraversión con la contratación gubernamental y se realicen en cumplimiento con la Ley de Ética Gubernamental, Ley 1-2012, según enmendada, y con el Título III de la Ley 2-2018, conocido como el Código de Ética para Contratistas Suplidores y Solicitantes de Incentivos Económicos del Gobierno de Puerto Rico.

4. ¿Qué tipo de contrato?
   a. Precio fijo (FFP), tiempo y materiales (T&M), otro
   b. ¿Fecha de adjudicación prevista? FY23 en lugar de FY24

   Se tiene previsto un contrato de servicios profesionales para la coordinación y elaboración de un plan de ciberseguridad. En dicho contrato, se acordará un precio por hora según la especialidad y/o el recurso. El contrato incluirá un límite máximo establecido.

E. Elementos Técnicos

1. ¿La propuesta se limita a solo los procesos en el Anejo II o puede abarcar otros procesos incluidos en un marco de referencia, tal como el NIST 800-53?

   Además de los requisitos mencionados en el Anejo III de la notificación PRITS 2023-001, el plan puede incluir otros procesos que contribuyan a mejorar los controles de seguridad en los sistemas de información. Esto puede involucrar la implementación de prácticas y estándares adicionales, como el NIST 800-53, entre otros.

2. Anejo III punto 1 – indica desarrollar un plan estratégico para reducir riesgos, ¿para esta identificación de riesgo podemos hacer un análisis de riesgo inicial con el framework NIST, es aceptable?

   Es requerido que plan estratégico sea desarrollado utilizando el marco de ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés) y el Marco de Iniciativa Nacional para la Educación en Ciberseguridad (NICE, por sus siglas en inglés.

3. Anejo III sección B bajo 1. F. iii – indica mejorar la preparación, respuesta y resistencia, ¿tienen actualmente un Incident Response Plan a mejorar?

   Dentro de las medidas de respuesta implementadas, se ha creado una guía y herramienta para reportar incidentes de ciberseguridad. Esta guía puede ser revisada, mejorada e incorporada como uno de los elementos a tener en cuenta en el plan de ciberseguridad y en el plan de gestión de incidentes.

4. ¿Puede PRITS proporcionar detalles adicionales o aclaraciones sobre lo que se entiende y se requiere con respecto a una "Declaración de seguridad y privacidad"?

La declaración de seguridad y privacidad a incluir en el plan debe establecer los principios, objetivos, políticas, estándares y controles necesarios para salvaguardar la información y garantizar el cumplimiento de las regulaciones y leyes de privacidad aplicables. La misma debe reconocer la importancia de proteger tanto la confidencialidad, integridad y disponibilidad de la información, como los derechos y la privacidad de los individuos cuyos datos se encuentran bajo custodia del Gobierno de Puerto Rico. Esta declaración abarca diversos aspectos como la clasificación de información, el acceso y control de privilegios, la gestión de incidentes, la evaluación de riesgos, la protección de datos personales y cualquier otro elemento relevante para asegurar la seguridad y privacidad de los datos gubernamentales.

5. ¿Puede PRITS proporcionar aclaraciones sobre a qué se aplica el servicio de "gestión, control y coordinación"; se refiere a la gestión, control y coordinación de actividades relacionadas con el desarrollo del Plan Estratégico de Ciberseguridad y/o otras actividades?

   La solicitud de servicios abarca la gestión, control y coordinación de actividades relacionadas con las evaluaciones iniciales necesarias para el desarrollo del plan, así como la creación del plan en sí mismo. Además, incluye la realización de adiestramientos, incluyendo la campaña de educación y diseminación del plan, y la organización de ejercicios para evaluar la efectividad de este.

F. Experiencia

1. Anejo II Sección A punto 3 – indica que se debe tener experiencia de mínimo tres (3) años, ¿Las experiencias son en territorio US o se puede incluir experiencias internacionales?

   Se requiere que los proponentes cuenten con experiencia en la prestación de servicios similares a los solicitados en términos de alcance, independientemente de la ubicación geográfica. Esta experiencia debe ser cónsona con la doctrina del Sistema Nacional de Manejo de Incidentes (NIMS, por sus siglas en inglés), el marco de ciberseguridad del NIST y otras regulaciones federales relacionadas con la ciberseguridad.

2. Anejo II Sección A punto 4 – indica que debemos presentar tipos de informes de clientes previos, por tratarse de información confidencial, ¿pueden ser “templates” de reportes?

   Se requiere que los informes solicitados de clientes anteriores sean originales. No obstante, se aceptarán documentos redactados que excluyan información confidencial.

G. Precios

1. Sobre la campaña de phishing para detectar vulnerabilidades de los usuarios: ¿Cuántos usuarios de correo electrónico se deben incluir en el servicio o prefiere un costo por el servicio entero y un precio general por campaña?

   Las campañas de phishing deben incluirse como parte del plan. Su implementación no está contemplada en los servicios solicitados en la notificación PRITS 2023-001.

2. Los precios de nuestros competidores no son públicos; ¿cómo podemos satisfacer la sección E de página 19 de esta solicitud?

   En la industria de IT, es común encontrar un rango de precios para la provisión de servicios similares. Se espera que los proponentes realicen un análisis de sus costos y establezcan precios competitivos que les permitan cubrir sus gastos y obtener beneficios razonables.

H. Propuesta

1. ¿Existe un límite máximo de páginas para la propuesta escrita?

   No hay una restricción en cuanto al número de páginas para la propuesta. Sin embargo, se recomienda que sea lo más clara y concisa posible.

2. ¿Tendremos oportunidad de realizar una presentación para abundar sobre los servicios propuestos y aclarar dudas suyas?

   Después de revisar las propuestas recibidas, PRITS se reserva el derecho de contactar a los proponentes para aclarar cualquier información proporcionada en la propuesta.

3. ¿Se pueden enviar propuestas en inglés, o en combinación de inglés y español?

   Las propuestas pueden ser presentadas en inglés. Si se presentaran en español, los conceptos de IT y/o vocabulario técnico podrían presentarse en inglés.

4. ¿Se pueden hacer propuestas juntas entre corporaciones con fines de lucro y corporaciones sin fin de lucro como parte de un acuerdo en grupo?

   No se aceptarán propuestas grupales.

5. ¿Las propuestas enviadas tienen que cubrir todos los aspectos del Anejo III por una sola compañía, o grupos de compañías?

   Cada compañía debe presentar su propuesta por separado. No se aceptarán propuestas grupales.

6. ¿Publicara PRITS información acerca de las compañías que respondan a la solicitud de preguntas para esta propuesta?

Una vez que PRITS efectúe la adjudicación correspondiente, notificará su determinación final en un Aviso de Adjudicación. El Aviso de Adjudicación incluirá los nombres de los Proponentes que participaron en la notificación de necesidad de servicios profesionales PRITS 2023-001, un resumen de sus propuestas y los factores o criterios considerados para la adjudicación de la propuesta.

7. Contenido de la propuesta, punto h (Pág. 9): Dirección física y postal de la oficina… ¿Requieren esa información en algún documento o formato específico, o se puede incluir toda la información requerida en la carta de presentación?

   No es necesario seguir un formato particular para presentar esta información, aunque se recomienda sea incorporada como un apéndice de la propuesta.

I. Recursos

1. ¿Podemos entender que estimar recursos por hora es suficiente en algunos casos?

   Las propuestas deben incluir el costo por hora por recurso para todos los servicios solicitados.

J. Seguros

1. Dado que el valor total y el número de personal del contrato no están decididos, ¿pueden los proponentes utilizar una póliza de seguro de responsabilidad civil general que permita agregar al personal que llevará a cabo el trabajo una vez que se haya adjudicado el contrato?

   Una vez que se haya adjudicado el contrato, se permite la inclusión del personal encargado de realizar el trabajo en una póliza de seguro de responsabilidad civil general.

2. Existe un requerimiento de póliza de seguro en la sección 2.8, ¿qué cantidad mínima debe cubrir por la póliza de seguro?

   Póliza de responsabilidad pública/comercial por la suma agregada general de no menor de $2,000,000.00, la cual debe incluir cobertura por cada ocurrencia con límite de no menor de $1,000,000.00.

K. Otros

1. Análisis de los riesgos que podrían representar una amenaza para los recursos críticos o esenciales, equipos, sistemas, archivos e instalaciones.
   P: ¿Existe una instalación/equipo SOC (Centro de Operaciones de Seguridad) preexistente? ¿O será necesario contar con una nueva instalación/equipo SOC?

El diseño pre-construcción del SOC está en curso y se llevará a cabo simultáneamente a los servicios solicitados en la notificación PRITS 2023-001.

2. Anejo II Sección D punto 2 – indica presentar servicios en plan de trabajo mensual por fases, ¿a cuánto tiempo requieren el plan? ¿Alguna metodología específica o de preferencia PMI, PRINCE2?

   La fecha límite para presentar el borrador final del plan es el 1 de agosto de 2023. Sin embargo, se proyecta que la implementación del plan se extienda a lo largo de 3 años.

   La metodología de preferencia para PRITS es PMI, pero los proponentes tienen la opción de presentar otra metodología y explicar cómo la misma favorece el desarrollo de plan.

3. ¿Puede PRITS proporcionar aclaraciones sobre a qué se aplica el servicio de "organización y asignación de responsabilidades"? ¿Se refiere a la organización y asignación de responsabilidades relacionadas con el desarrollo del Plan Estratégico de Ciberseguridad y/o otras actividades?

   El plan estratégico debe abordar la organización y asignación de responsabilidades tanto desde la perspectiva de la gobernanza como de la implementación del plan. En la medida de lo posible, se deben describir las responsabilidades de las entidades gubernamentales en la implementación del plan. Asimismo, es fundamental contemplar la capacitación adecuada en ciberseguridad al personal de acuerdo con sus responsabilidades, para que cuenten con los conocimientos y habilidades necesarios para identificar los riesgos de ciberseguridad y comprender sus roles y responsabilidades dentro de las políticas, procedimientos y prácticas establecidos en materia de ciberseguridad.

4. ¿Existen plazos especificados en la notificación para el Plan Estratégico de Ciberseguridad; sin embargo, se proporcionarán plazos para otros servicios especificados en el Anexo III (por ejemplo, "Pruebas de penetración para todas las conexiones internas y externas", "Monitoreo y análisis de eventos sospechosos", "Procedimientos operativos estándar (SOP) para la detección, respuesta y contención de incidentes", "Campaña de phishing para detectar vulnerabilidades de los usuarios", "Actualización, mejora y políticas de parches")? ¿O los plazos para esos otros servicios se establecerán y acordarán con un Proponente(s) al que se le adjudique un contrato de conformidad con esta notificación (es decir, "Proponente Afortunado") más adelante durante el proceso de negociación del contrato y/o al inicio del contrato?

   Los plazos concretos de esta solicitud de servicios se indicaron en el Anejo III de la Notificación PRITS 2023-001. Los plazos para los demás servicios serán acordados con el(los) Proponente(s) Agraciado(s).

5. ¿Es la fecha límite de aprobación de este Plan, el 30 de septiembre de 2023, la fecha límite para que PRITS y/o el Comité de Planificación de Ciberseguridad de Puerto Rico

aprueben el Plan, ya que es la misma fecha límite para enviar el Plan a CISA para su revisión?

La fecha límite para la aprobación del plan por parte del Comité de Ciberseguridad es el 30 de septiembre de 2023.

6. ¿Puede PRITS proporcionar aclaraciones sobre lo que se requiere para realizar el servicio de "gestión de datos sensibles" y cómo esto involucrará la Ley Patriota (Patriot Act)?

   La Ley "Patriot Act" confiere al gobierno de los Estados Unidos poderes en términos de recopilación, acceso y vigilancia de información para la prevención y persecución de actividades terroristas, así como información relevante para la seguridad nacional. En términos de los datos sensibles, es necesario establecer controles que permitan cumplir con esta ley sin comprometer la protección de los datos personales y sensitivos de los individuos, evitando el acceso por personal no autorizado. Es imprescindible evaluar cuidadosamente el almacenamiento y procesamiento de datos sensibles para garantizar el cumplimiento de las leyes de protección de datos aplicables y preservar la privacidad de los individuos.

7. ¿Se pueden realizar todos o algunos de los servicios proporcionados de conformidad con la notificación de forma remota/virtual? En caso afirmativo, ¿puede PRITS especificar qué servicios, y en qué medida, se pueden realizar de forma remota/virtual?

   Algunos de los servicios solicitados pueden ser realizados de manera remota. Es responsabilidad de los proponentes indicar en sus propuestas qué servicios planean llevar a cabo de forma remota, así como la cantidad de horas que se dedicarán en esta modalidad.

   Sin embargo, se espera que el proponente agraciado esté disponible de manera presencial cuando le sea requerido. Los detalles específicos sobre la frecuencia y la duración de estas reuniones presenciales se comunicarán directamente al proponente una vez que haya sido seleccionado.

8. ¿Se publica también la solicitud en inglés? En caso afirmativo, ¿puede proporcionar la URL directa?

   La notificación de solicitud de servicios profesionales PRITS 2023-001 sólo se encuentra disponible en español.

9. ¿Cuál es el papel de la Autoridad de Alianza Público-Privadas de Puerto Rico (P3A) y la evaluación de los servicios delegados a la industria privada como parte de este SOW?

La Autoridad de Alianzas Público-Privadas no participa en la notificación de solicitud de servicios ni se encarga de la contratación o evaluación de los servicios objeto de esta notificación.

10. ¿Cuál es la demarcación entre PRITS y DSP en términos de autoridades para el desarrollo de soluciones, implementación, cumplimiento y respuesta?

    El Departamento de Seguridad Pública (DSP) y PRITS mantienen una colaboración para la reducción de los riesgos cibernéticos y enfrentar desafíos gubernamentales específicos. Sin embargo, la responsabilidad de gestionar, implementar y evaluar las iniciativas relacionadas con los sistemas de información y ciberseguridad a nivel gubernamental recae en la Oficina del PRITS.

L. Preguntas fuera del alcance de la solicitud de servicios profesionales

La notificación de necesidad de servicios profesionales número PRITS 2023-001 "Para establecer contratos para la coordinación y desarrollo de un plan de ciberseguridad" se centra en la creación de un plan que permita al Gobierno prepararse y responder a futuros incidentes de ciberseguridad. El enfoque principal es proteger sus redes y sistemas de información, así como el adiestramiento del personal gubernamental y de aquellas entidades que manejan sistemas de información en nombre del Gobierno de Puerto Rico.

Los dieciocho elementos presentados al principio del Anejo III de la notificación PRITS 2023-001 deben ser considerados como parte integral del plan estratégico de ciberseguridad. Los proponentes no deben incluir la implementación de estos elementos como parte de los servicios a ofrecer. Para obtener más detalles sobre los requisitos de los servicios solicitados refiérase a la sección "Especificaciones del servicio" del Anejo III del Aviso.

Conforme a lo establecido anteriormente, las preguntas planteadas a continuación se consideran fuera del alcance de los servicios solicitados en esta etapa y, por ende, no se proporcionarán respuestas.

1. ¿Cuál es el alcance para el análisis, pruebas y plan en términos de cantidad de Agencias, cantidad de direcciones IP internas y direcciones IP externas?

2. ¿Se desea limitar el número de direcciones IP o activos conectados a la red interna y externa a una cantidad especifica o se desea incluirlo todo en el alcance?

3. ¿Se desea incluir un enfoque en algún sistema de información o aplicación en específico o las pruebas quieren que sean generales?

4. Favor de abundar sobre el alcance de este servicio incluyendo requerimientos sobre:
    a. ¿Clasificación de datos y *labeling*?
    b. ¿Cifrado en transmisión y resguardo?

c. Detección y prevención de exfiltración de datos (DLP) a nivel de: ¿Correo electrónico, servidores, bases de datos o transmisión?
d. Monitoreo de Integridad de Archivos (FIM)
e. Control de Acceso granular

5. ¿Favor de abundar en el alcance del servicio (infraestructura, frecuencia de verificación o ajuste, continuo (*self-healing*)?

6. Favor de proveer la cantidad de dispositivos de red y servidores que se desean monitorear e incorporar configuraciones seguras. ¿Cuál desea sea el alcance en el monitoreo?, sistema operativo, base de datos, *firewalls*, WAF, EDR, AV, servidor HTTP, entre otros.

7. Anejo III punto 3 – indica que se deben incluir pruebas de penetración a todas las conexiones internas y externas – ¿Podrán brindar la siguiente información? (Indique marca/modelo/versiones, cuando aplique)
    a. Cantidad de IPs externos
    b. Cantidad de IPs internos
    c. Cantidad de WiFi SSIDs
    d. Cantidad de WebApps
    e. Cantidad de servicios nube a ejecutar pruebas de penetración
    f. Cantidad y tipo de sistemas operativos
    g. Cantidad y tipo de navegadores web
    h. Cantidad de servidores de bases de datos
    i. Cantidad y tipo de herramientas de seguridad
    j. Cantidad de servidores de correo electrónico
    k. Cantidad de dispositivos de red, *firewalls*, *routers*, *switches*, *ipsec tunnels* y cantidad de tráfico
    l. Cantidad de usuarios / *endpoints*
    m. Recurrencia de estas pruebas

8. ¿Alguna adversidad sobre soluciones implementadas en las nubes privadas (Azure, AWS, por ejemplo)?

9. ¿Requiere servicios sobre el manejo de control de acceso o administración de sistemas de información conducentes a la administración de su seguridad?

10. ¿La propuesta se limita a solo los procesos en el Anejo II o puede abarcar otros procesos incluidos en un marco de referencia, tal como el NIST 800-53?

11. ¿Cuáles serían los protocolos aceptados a utilizar para monitoreo: WMI, SNMP, API?

12. ¿Tienen algún estándar implementado para la normalización de logs o requerimientos mínimos para la integración con un sistema de manejo de información de seguridad y eventos (SIEM) o un VSOC?

13. ¿Qué aspectos de su infraestructura desea incluir en el monitoreo (Dispositivos de seguridad perimetral, enrutamiento y redes, servidores, estaciones de trabajo, bases de datos, sistemas operativos, Hypervisors, etc.)?

14. ¿Favor de abundar en cuanto al apoyo en servicios de respuesta a incidentes, requiere de intervención nuestra para la contención y luego remediación o solo notificación, priorización de riesgo (o todas las anteriores)?

15. ¿Cuál sistema de correo electrónico utilizan, O365, Outlook on prem, otros? De ser O365, ¿qué licenciamiento tienen actualmente? ¿Cuántos buzones tienen actualmente?

16. ¿Requiere se incluya la verificación de vulnerabilidades (en adición a parches) por medio de escaneos autenticados o soluciones de detección de postura de seguridad?

17. ¿Actualmente se utiliza una herramienta de parches y políticas actuales? ¿O se estará trabajando con implementación de una herramienta de parches nueva y creación de políticas?

18. ¿Incluye parches a las aplicaciones de terceros o centrado en publicaciones a nivel de sistema operativo?

19. Anejo III punto 6 – indica monitoreo y análisis de eventos sospechosos, ¿cuentan con una plataforma SIEM? Si no, ¿cuánta es la cantidad de eventos a nivel Gb por día que estaremos contemplando en propuesta para ingesta?

20. Anejo III punto 9 – indica crear SOPs para detección, respuesta y contención de incidentes, ¿qué herramientas están implementadas actualmente para que sean parte de este SOP?

21. Anejo III sección B bajo 1. E. vi. – indica capacidad de reconstruir sistemas, ¿cuáles serían los *workloads* a hacer *backup* y reconstruir? ¿Qué cantidad de TBs por workload?

22. ¿Puede PRITS proporcionar detalles adicionales sobre los tipos de datos sensibles que requieren protección y dónde y cómo se almacena, utiliza y transmite esa información?

23. ¿Puede PRITS proporcionar una estimación del número y tipos de servidores de correo y clientes de correo que se dirigirán para mejorar la protección del correo electrónico?

24. ¿Existen procedimientos operativos estándar u otros planes o políticas, etc., ya existentes para la detección, respuesta y contención de incidentes? En caso afirmativo, ¿es intención de PRITS que el Proveedor al que se le adjudique el contrato para realizar los servicios actualice esos planes, políticas, etc., existentes o cree nuevos procedimientos operativos estándar para la detección, respuesta y contención de incidentes?

25. ¿Puede proporcionar una descripción general de la arquitectura a alto nivel?
    a. ¿Cuántos puntos de acceso a Internet (IAP) respaldan la GovPRNet?
    b. ¿Hay una suite de ciberseguridad consolidada en los IAP?
    c. ¿Cuántos nodos de entrega de servicios hay?
    d. ¿Número total estimado de usuarios y dispositivos de todo tipo?
    e. ¿Hay un NOC/SOC/IRT consolidado y un SLA con el Equipo de Ciberseguridad de PRNG?
    f. Seguimiento de 7 sitios de aterrizaje de cables submarinos en PR. (16 cables, 4 sitios de aterrizaje en SJ, 1/1 en Aguadilla, 1/1 en Humacao, 1/1 en Ponce) g. ¿Cuál es la colaboración/coordinación con los propietarios del servicio de transmisión de cables?
    g. ¿Está GovPR suscrito a un ISP de SATCOM de emergencia o tiene un plan de contingencia en caso de que los sitios de aterrizaje de cables se vean afectados?

Anejo I:

The Department of Homeland Security Notice of Funding Opportunity Fiscal Year 2022 State and Local Cybersecurity Grant Program[1]

Appendix C: Cybersecurity Plan

Cybersecurity Plan Basics

- Comprehensive strategic plan to reduce cybersecurity risk and increase capability across the entity
- Entity-wide plan, not a single entity
- Should cover 2 to 3 years
- Must include required elements, with discretion to add other
- elements as necessary
- Existing plans can be utilized
- There is no required template, but required elements must be
- identifiable for review purpose
- Individual projects must align to Cybersecurity Plan
- Must be approved by the Cybersecurity Committee and
- CIO/CISO/Equivalent
- CISA approves for DHS
- Plans are initially approved for 2 years; annually thereafter

Submission of a Cybersecurity Plan is required for any eligible entity participating in the State and Local Cybersecurity Grant Program (SLCGP). The Cybersecurity Plan is a key component of a strategic approach to building cyber resilience. The Cybersecurity Planning Committee, with a holistic membership representing the various stakeholder groups across the entity, is responsible for developing, approving, revising, and implementing the Cybersecurity Plan.

Accordingly, the Cybersecurity Plan should establish high level goals and finite objectives to reduce specific cybersecurity risks at SLT governments across the eligible entity. The Cybersecurity Plan should also serve as the overarching framework for the achievement of the SLCGP goal, with grant-funded projects working to achieve outcomes. Regional approaches, as part of an entity-wide approach, should also be considered.

In developing the Cybersecurity Plan, the Cybersecurity Planning Committee should consider the following:

- Existing governance and planning documents and identification of any planning gaps that should be addressed by the Cybersecurity Plan;

[1] Fuente: https://www.fema.gov/fact-sheet/department-homeland-security-notice-funding-opportunity-fiscal-year-2022-state-and-local

- Existing assessments and evaluations (e.g., reports, after action reports) conducted by SLT governments within the entity and any planning gaps that require additional assessments and/or evaluations; and
- Identification of potential SLCGP projects to address planning gaps and prioritize mitigation efforts.

Plan Components

- Roles and responsibilities
- Required elements
- Discretionary elements
- Capabilities assessment
- Implementation plan
- A summary of projects
- Metrics

Cybersecurity Plan Overview

The following identifies the overall plan requirements and additional considerations that eligible entities should consider when constructing the Cybersecurity Plan. Although there is no required format for the Cybersecurity Plan, Cybersecurity Planning Committees are encouraged to review the Cybersecurity Plan Template, which includes additional details, samples, and templates.

Cybersecurity Plans must include and address the following items:

- Incorporate, to the extent practicable, any existing plans to protect against cybersecurity risks and cybersecurity threats to information systems owned or operated by, or on behalf of, SLTs. Building upon and incorporating existing structures and capabilities allows entities to provide governance and a framework to meet the critical cybersecurity needs across the entity while making the best use of available resources. For example, consider referencing an existing emergency management plan to address potential downstream impacts affecting health and safety when responding to or recovering from a cybersecurity incident.
- Describe how input and feedback from local governments and associations of local governments was incorporated. For states, the SLCGP is intended to reduce cybersecurity risk across the eligible entity. Incorporating input from local entities is critical to building a holistic Cybersecurity Plan.
- Include the specific required elements (see Required Elements section of this Appendix below). There are 16 required elements that are central to the Cybersecurity Plan and represent a broad range of cybersecurity capabilities and activities. They also include specific cybersecurity best practices that, when implemented over time, will substantially reduce cybersecurity risk and cybersecurity threats. While each of the 16 required elements must be addressed

in the plan, this may include a brief explanation as to why certain elements are not currently being prioritized. Not all 16 elements are required to be aligned to projects and have associated funding. These determinations should be addressed in accordance with capability gaps and vulnerabilities identified through an objective assessment process.

- Describe, as appropriate and to the extent practicable, the individual responsibilities of the state and local governments within the state in implementing the Cybersecurity Plan. Defining the roles and responsibilities of SLT governments is critical from both governance and implementation perspectives.
- Assess the required elements from an entity-wide perspective. The candid assessment of the current capabilities of SLT entities is the first step in reducing cybersecurity risk across the entity. This assessment also serves as the justification for individual projects. Additional information on the assessment is provided below and in the Cybersecurity Plan Template.
- Outline, to the extent practicable, the necessary resources and a timeline for implementing the plan. The Cybersecurity Plan is a strategic planning tool that looks two to three years into the future. Accordingly, it should map how the Cybersecurity Planning Committee seeks to achieve plan goals and objectives. Cybersecurity Plans should address how SLCGP funds will help develop and/or implement the plan. It should also map how other activities and funding sources contribute to the achieving the outcomes described in the plans.
- Summary of associated projects. Individual projects are the way elements of the plan are implemented over time. The plan must include a summary of projects associated with each required and discretionary element, designating which will use SLCGP funds. Details for each project using SLCGP funds must be included in the Investment Justification.
- Describe the metrics that the eligible entity will use to measure progress. The metrics that will be used must measure implementation of the Cybersecurity Plan and, more broadly, cybersecurity risks reduction across the state. These are different than the metrics that will be used to measure outcomes of the SLCGP, as described in Section A.10-A.11 and Appendix A of this NOFO. Additional information is provided in the Cybersecurity Plan Metric Section below and also in the Cybersecurity Plan Template.
- Approvals - the Cybersecurity Plan must be approved by the Cybersecurity Planning Committee and the CIO/CISO/Equivalent. The eligible entity, upon submitting the Cybersecurity Plan, must certify that the Cybersecurity Plan has been formally approved by the Cybersecurity Planning Committee and the CIO/CISO/Equivalent of the eligible entity.

Cybersecurity Planning Committees should also consider the following when constructing the Cybersecurity Plan:

- Holistic approach to the Cybersecurity Plan. The Cybersecurity Plan should be strategic in nature, guiding development of capabilities to address cybersecurity risks and threats across the state or territory. Individual projects should

demonstrably support the state, territorial, and local entities in achieving those capabilities over time.

- Focused investments that are sustainable over time. The SLCGP currently is authorized for four years and limited funds are available. Cybersecurity Plans must address how SLT entities will sustain capabilities once the program ends or funds are no longer available.
- State role as leader and service provider. Many states have significant cyber defenses and elect to provide services to local entities to improve capabilities. Where appropriate, states should consider approaches to support state-wide efforts, that may include using funds to provide services to local entities. Multientity projects are another way that eligible entities can group together to address cybersecurity risk and build capabilities (See Appendix D for additional information on multi-entity activities).
- Building from existing efforts. Cybersecurity Committees should consider describing how cooperative programs developed by groups of local governments are integrated into the entity-wide approach.
- Additional cybersecurity elements prioritized by the Cybersecurity Planning Committee.

Required Cybersecurity Best Practices

Although these cybersecurity best practices must be addressed in the Cybersecurity Plan, immediate adoption by every SLT entity is not required. Cybersecurity Plans must clearly articulate efforts to implement these cybersecurity best practices across the eligible entity within reasonable timelines. Individual projects that assist SLT entities adopt these best practices should also be prioritized by the Cybersecurity Planning Committee. As there are multiple ways to implement the best practices, this approach provides committees the flexibility to work with SLT entities to design a plan that takes resource constraints, existing programs, and other factors into account.

Required Elements

If there are any existing plans that meet the required elements, references to them may be used in lieu of incorporating them in their entirety. The Cybersecurity Plan must describe, to the extent practicable, how the state plans to address the below elements. The Cybersecurity Plan is a strategic document, looking broadly across the entire jurisdiction. The description should support the vision, mission and other strategic guidance set by the Cybersecurity Planning Committee.

1. Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology.

2. Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.

3. Enhance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, against cybersecurity risks and cybersecurity threats.

4. Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.

5. Ensure that the state or local governments within the state, adopt and use best practices and methodologies to enhance cybersecurity, discussed further below.

The following cybersecurity best practices under required element 5 must be included in each eligible entity's Cybersecurity Plan:

- Implement multi-factor authentication;
- Implement enhanced logging;
- Data encryption for data at rest and in transit;
- End use of unsupported/end of life software and hardware that are accessible
- from the Internet;
- Prohibit use of known/fixed/default passwords and credentials;
- Ensure the ability to reconstitute systems (backups); and
- Migration to the .gov internet domain.

Additional best practices that the Cybersecurity Plan can address include:

- The National Institute of Standards and Technology (NIST) Cybersecurity
- Framework;
- NIST's cyber chain supply chain risk management best practices; and
- Knowledge bases of adversary tools and tactics.

6. Promote the delivery of safe, recognizable, and trustworthy online services by the state or local governments within the state, including through the use of the .gov internet domain.

7. Ensure continuity of operations of the state or local governments within the state, in the event of a cybersecurity incident, including by conducting exercises to practice responding to a cybersecurity incident.

8. Use the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by NIST to identify and mitigate any gaps

in the cybersecurity workforces of the state or local governments within the state, enhance recruitment and retention efforts for those workforces, and bolster the knowledge, skills, and abilities of personnel of the state or local governments within the state, to address cybersecurity risks and cybersecurity threats, such as through cybersecurity hygiene training.

9. Ensures continuity of communication and data networks within the jurisdiction of the state between the state and local governments within the state in the event of an incident involving those communications or data networks.

10. Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the jurisdiction of the state.

11. Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.

12. Leverage cybersecurity services offered by the Department (See Appendix G for additional information on CISA resources and required services and membership).

13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives.

14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats. Local governments and associations of local governments within the state should be consulted. Cybersecurity Planning Committees should also consider consulting neighboring entities, including adjacent states and countries.

15. Ensure adequate access to, and participation in, the services and programs described in this subparagraph by rural areas within the state.

16. Distribute funds, items, services, capabilities, or activities to local governments.

Cybersecurity Planning Committees are strongly encouraged to expand their Cybersecurity Plans beyond the required elements. This may include a focus on specific critical infrastructure or emphasis on different types of SLT entities.

Required Capabilities Assessment

Given the Cybersecurity Plan is a strategic document, it should not identify

specific vulnerabilities but instead capture the broad level of capability across the jurisdiction. The assessment will become the road map for individual projects and activities using SLCGP funds. All Investment Justifications must reference the capability gaps identified in the assessment. The Cybersecurity Plan Capabilities Assessment Worksheet (see Cybersecurity Plan Template) provides an easy way for Cybersecurity Planning Committees to capture this information and can be customized as appropriate.

Summary of Projects

Although the Cybersecurity Plan is a strategic document, it must show how individual projects and activities will implement the plan over time. A summary of projects using FY 2022 SLCGP funds associated with each required and discretionary element provides a helpful snapshot of state- and territory-wide capability and capacity that will be achieved as a result of this funding. Details for each project using SLCGP funds must be included in Investment Justification (see Appendix F) and is to include a description of the purpose of the project and what it will accomplish, and, more specifically, how the project will address an identified gap or need and how it supports one or more of the required elements.
The Cybersecurity Plan Template includes a fillable Project Plan Worksheet, a sample of which is below.

- Column 1. Project number assigned by the entity
- Column 2. Name the project
- Column 3. Brief (e.g., 1-line) Description of the purpose of the project
- Column 4. The number of the Required Elements the project addresses
- Column 5. Estimated project cost
- Column 6. Status of project (future, ongoing, complete)
- Column 7. Project priority listing (high, medium, low)
- Column 8. Project Type (Plan, Organize, Equip, Train, Exercise)]

Sample Table – Project Plan Worksheet

1.#	2.Project Name	3.Project Description	4.Related Required Element #	5.Cost	6.Status	7.Priority	8.Project Type

Cybersecurity Plan Metrics

Cybersecurity Plans must include language detailing how the state will measure

both: 1) how the state will implement the plan; and 2) how the state will reduce cybersecurity risks to, and identify, respond to, and recover from cybersecurity threats to, information systems owned or operated by, or on behalf of, the state or local governments within the state. These measures should be at the macro level, related to the goals, objectives, and priorities as part of the overarching strategic plan and not associated with individual projects. See page 6 of this NOFO for additional information on required metrics and reporting.
States, and their Cybersecurity Planning Committees in helping with Cybersecurity Plans, should consider the following when developing metrics:

- Aligning metrics to the Cybersecurity Plan and the established program goals and objectives included at Appendix A.
- Reviewing existing metrics that are in use across the state; and
- The data for each metric must be available and reportable and should not create unnecessary burdens to collect.