Ispettorato nazionale per la sicurezza nucleare e la radioprotezione
Il Direttore

Determina n.69 del 24/ 04 /2024

OGGETTO: DELEGA AL SEGRETARIO GENERALE DELLE FUNZIONI ASSUNTE DAL DIRETTORE IN SOSTITUZIONE DEL DIRIGENTE DEL SERVIZIO AGBP PER L'ISTRUTTORIA, LA VALUTAZIONE E L'EROGAZIONE DA PARTE DELL'AGENZIA PER LA CYBERSICUREZZA NAZIONALE (DI SEGUITO ACN) DEI SERVIZIO PER IL POTENZIAMENTO E IL MIGLIORAMENTO DELLA CAPACITÀ CYBER DELL'ISIN DI CUI AVVISO PUBBLICO N. 7/2023, NOMINA DEL RESPONSABILE DEL RELATIVO PROCEDIMENTO AI SENSI DELLA LEGGE N. 241 DEL 1990 E DEI RESPONSABILI TECNICI, PER L'ESECUZIONE, L'ATTUAZIONE E L'ADEMPIMENTO DEGLI OBBLIGHI STABILITI DALLO SCHEMA DI CONVENZIONE TRASMESSA DA ACN E ALLEGATA CON LA RELATIVA SCHEDA DI INTERVENTO AL PRESENTE PROVVEDIMENTO.

IL DIRETTORE DELL'ISPETTORATO NAZIONALE PER LA SICUREZZA NUCLEARE E LA RADIOPROTEZIONE

VISTO il Decreto legislativo 4 marzo 2014, n. 45, come modificato dal decreto legislativo 15 settembre 2017, n. 137 di recepimento della direttiva 2011/70/EURATOM, e 2014/87EURATOM e in particolare gli articoli 1, 6 e 9 che istituiscono l'Ispettorato Nazionale per la Sicurezza Nucleare e la Radioprotezione con funzioni e compiti di autorità nazionale di regolazione in materia di sicurezza nucleare e radioprotezione;

VISTO il Regolamento di organizzazione e funzionamento interni dell'ISIN approvato con delibera del Direttore dell'ISIN n. 3 del 22 giugno 2018, prot. n. 1061 del 25 giugno 2018, e modificato con delibere del Direttore dell'ISIN n. 5 del 22 febbraio 2021 e n. 3 del 15.11.2023;

CONSIDERATO che l'ISIN con determina 19/01/2024 dell'Agenzia per la Cybersicurezza Nazionale è stato ammesso al servizio avente ad oggetto "*Interventi di potenziamento della resilienza cyber - PA Centrale*" di cui all'avviso pubblico 7/2023 finanziati con il PNRR per un importo complessivo massimo di € 637.500,00;

VISTA la Proposta di Convenzione dell'Agenzia per la Cybersicurezza Nazionale avente ad oggetto il servizio per il potenziamento e il miglioramento della capacità cyber dell'ISIN che,

corredata dalla scheda di intervento, è allegata sotto la lettera "A" alla presente determina di cui costituisce parte integrante e sostanziale;

VISTA la Legge 7 agosto 1990, n. 241 recante "*Nuove norme sul procedimento amministrativo*" e in particolare l'articolo 4 in base al quale <*il dirigente di ciascuna unità organizzativa provvede ad assegnare a sé o altro dipendente addetto all'unità la responsabilità dell'istruttoria e di ogni altro adempimento inerente il singolo procedimento nonché, eventualmente, dell'adozione del provvedimento finale.*> e <*fino a quando non sia effettuata* (tale) *assegnazione ……., è considerato responsabile del singolo procedimento il funzionario preposto alla unità organizzativa*> ;

VISTA la PEC del 29.3.2024 con la quale il dott. Claudio Nicolini, RUP del procedimento per l'istruttoria, il perfezionamento e l'esecuzione del menzionato progetto in oggetto in qualità di dirigente del Servizio AGBP, ha comunicato al Direttore dell'ISIN di voler essere sostituito;

VISTA la determina n. 45 del 04/04/2024, prot. n. 112461, con la quale il direttore dell'ISIN ha assunto temporaneamente le funzioni del dott. Claudio Nicolini per l'esame e le necessarie valutazioni istruttorie al fine dell'eventuale perfezionamento ed esecuzione del progetto per l'erogazione di interventi di potenziamento e di miglioramento delle capacità cyber di ISIN di cui all'avviso pubblico 7/2023, sollevandolo dalla funzione di responsabile unico del procedimento;

VISTO il verbale della Conferenza di Servizi istruttoria del 04.04.024, prot. n. 112888, convocata dal Direttore dell'ISIN con all'ordine del giorno i necessari approfondimenti istruttori del progetto di erogazione di interventi di potenziamento e di miglioramento delle capacità cyber di ISIN di cui all'avviso pubblico 7/2023;

VISTO il verbale della riunione del 12.04.2024, prot. n. 113545, svolta con ACN con all'ordine del giorno i necessari approfondimenti istruttori del progetto di erogazione di interventi di potenziamento e di miglioramento delle capacità cyber di ISIN di cui all'avviso pubblico 7/2023;

RILEVATO che all'esito degli approfondimenti effettuati nel corso delle menzionate riunioni è emerso che le attività oggetto del Servizio proposto da ACN di potenziamento e di miglioramento delle capacità cyber di ISIN di cui all'avviso pubblico 7/2023, risultanti dalla scheda di intervento allegata alla proposta di Convenzione allegata sub "A", non comporta una ulteriore spesa per le attività di vulnerability assessement già assicurate sui sistemi nell'ambito della Convenzione stipulata tra Unioncamere e ISIN;

RITENUTO pertanto di poter procedere all'approvazione e alla stipula della Convenzione allegata sub "A", che non comporta nuovi o ulteriori oneri a carico dell'amministrazione;

RITENUTO di delegare al Segretario Generale l'esercizio delle funzioni assunte dal Direttore in sostituzione del Dirigente del Servizio AGBP per l'istruttoria e l'attuazione dei servizi di potenziamento e di miglioramento delle capacità cyber di ISIN di cui all'avviso pubblico 7/2023, come specificato nella scheda di intervento allegata alla proposta di Convenzione allegata sub "A";

RITENUTO altresì di procedere alla nomina di un responsabile unico del procedimento ai sensi della legge n. 241 del 1990 e di due responsabili tecnici per garantire il necessario supporto al soggetto individuato da ACN di erogare i servizi per il potenziamento e il miglioramento delle

capacità cyber di ISIN di cui all'avviso pubblico 7/2023, come specificate nella scheda di intervento allegata alla proposta di Convenzione allegata sub "A";

VISTO il Decreto legislativo 8 marzo 2013, n. 39, recante "*Disposizioni in materia di inconferibilità e incompatibilità di incarichi presso le pubbliche amministrazioni e presso gli enti privati in controllo pubblico, a norma dell'articolo 1, commi 49 e 50, della legge 6 novembre 2012, n. 190*";

VISTO il Decreto del Presidente della Repubblica 16 aprile 2013, n. 62, rubricato "*Regolamento recante codice di comportamento dei dipendenti pubblici a norma dell'art. 54 del D.lgs. 30 marzo 2001, n. 165*";

RITENUTO che l'avv. Jacopo Maria Abruzzo è in possesso dei requisiti di esperienza e formazione professionale necessari per svolgere le funzioni di RUP del progetto avente ad oggetto l'erogazione da parte di ACN del servizio per l'attuazione di interventi di potenziamento e di miglioramento delle capacità cyber di ISIN di cui all'avviso pubblico 7/2023;

RITENUTO che l'ing. Giuseppe Cozzolino e l'ing. Matteo Spuri sono in possesso dei requisiti professionali di esperienza e di capacità tecnica necessari per garantire il necessario supporto tecnico al soggetto incaricato da ACN di effettuare le attività del servizio per il potenziamento e il miglioramento delle capacità cyber di ISIN di cui all'avviso pubblico 7/2023

DISPONE

1 di approvare la Convenzione e le relative attività individuate dalla scheda di intervento che la correda, allegata sotto la lettera "A", dando atto che la sottoscrizione della stessa non comporta nuovi o ulteriori oneri a carico del bilancio dell'ISIN;

2 di delegare al dott. Alessandro Carettoni le funzioni assunte dal Direttore in sostituzione del Dirigente del Servizio AGBP per l'istruttoria, la gestione e l'esecuzione del progetto avente ad oggetto l'erogazione da parte di ACN del servizio per l'attuazione di interventi di potenziamento e di miglioramento delle capacità cyber di ISIN di cui all'avviso pubblico 7/2023;

3 di nominare, l'avv. Jacopo Maria Abruzzo responsabile unico del procedimento avente ad oggetto l'erogazione da parte di ACN del servizio per l'attuazione di interventi di potenziamento e di miglioramento delle capacità cyber di ISIN di cui all'avviso pubblico 7/2023, come individuati nell'apposita scheda di intervento allegata allo schema di convenzione allegato sotto la lettera "A", dando atto che nell'espletamento dell'incarico è tenuto, in particolare, a seguire ed assicurare l'adempimento da parte di ISIN di tutti gli obblighi stabiliti nello schema di Convenzione allegata sub "A" di cui con riferimento alle prestazioni in oggetto, quale Responsabile unico del progetto (RUP), e a curare il corretto svolgimento delle procedure;

4 di nominare l'ing. Giuseppe Cozzolino e l'ing. Matteo Spuri, responsabili tecnici con il compito di assicurare il necessario supporto tecnico, in adempimento degli impegni posti a carico di ISIN nello schema di Convenzione allegata sub "A", e in tal modo consentire al soggetto incaricato da ACN di effettuare i servizi per il potenziamento e di miglioramento delle capacità cyber di cui all'avviso pubblico 7/2023, elencati nella scheda di intervento allegata alla menzionata convenzione;

5 di dare atto che il presente provvedimento entra in vigore dalla data di sottoscrizione;

6 di dare atto che gli incarichi di RUP e di responsabili tecnici sono svolti a titolo gratuito e non comportano nuovi o ulteriori oneri a carico del bilancio dell'ISIN;

7 di comunicare il presente provvedimento al Segretario Generale, al Dirigente del Servizio AGBP, al RUP e ai Responsabili tecnici;

8 di trasmettere il presente provvedimento al Responsabile per la prevenzione della corruzione e la trasparenza per la pubblicazione sul sito web dell'ISIN.

Avv. Maurizio Pernice

Maurizio Pernice
24.04.2024
13:05:44
GMT+01:00

Finanziato dall'Unione europea NextGenerationEU

DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

Allegato A

AVVISO PUBBLICO 7/2023

a sportello per l'erogazione di interventi di potenziamento e di miglioramento delle capacità cyber degli Organi costituzionali e di rilevanza costituzionale, dei Ministeri, delle Agenzie Fiscali, degli Enti di regolazione dell'attività economica, delle Autorità amministrative indipendenti e degli Enti a struttura associativa

PIANO NAZIONALE DI RIPRESA E RESILIENZA, Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity"

M1C1I1.5

ALLEGATO C – SCHEMA DI CONVENZIONE

Accordo di concessione del servizio finanziato

Per la regolamentazione dei rapporti di attuazione, gestione e controllo relativi all'erogazione degli interventi di cui alla istanza di partecipazione n. 31079 del 05/12/2023 ammessa con graduatoria approvata con determina protocollo n. 1841 del 19/01/2024 - CUP F84E21007910007;

tra

L'Agenzia per la Cybersicurezza Nazionale (C.F. 96501130585), con sede legale a Roma (RM), in Via di Santa Susanna n. 15 – cap. 00187, rappresentata dal Direttore Generale Bruno Frattasi, in qualità di legale rappresentante (di seguito **"Soggetto attuatore" o "Agenzia")**

e

Il _____ (C.F./P.IVA _____) rappresentata dal _____ in qualità di organo titolare del potere di impegnare l'Amministrazione _____ con sede legale a _____ (___) in Via/Piazza _____ n. ___ Cap _____ (di seguito **"Soggetto destinatario")**

di seguito congiuntamente definite le **"Parti"**

VISTO

- la legge 7 agosto 1990, n. 241, recante *"Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi"*, e, in particolare, l'articolo 12, secondo cui la concessione di sovvenzioni, contributi, sussidi ed ausili finanziari e l'attribuzione di vantaggi economici di qualunque genere a persone ed Enti pubblici e privati sono subordinate alla predeterminazione da parte delle Amministrazioni procedenti, nelle forme previste dai rispettivi ordinamenti, dei criteri e delle modalità cui le amministrazioni stesse devono attenersi;
- il decreto legislativo 31 marzo 2023, n. 36, recante *"Codice di contratti pubblici in attuazione dell'art. 1 della legge 21 giugno 2022, n. 78, recante delega al governo in materia dei contratti pubblici"*;
- il Regolamento (UE, Euratom) 2018/1046 del Parlamento europeo e del Consiglio del 18 luglio 2018, che stabilisce le regole finanziarie applicabili al bilancio generale dell'Unione, che modifica i Regolamenti (UE) n. 1296/2013, n. 1301/2013, n. 1303/2013, n. 1304/2013, n. 1309/2013, n. 1316/2013, n. 223/2014, n. 283/2014 e la decisione n. 541/2014/UE e abroga il Regolamento (UE, Euratom) n. 966/2012;
- il decreto legislativo 18 maggio 2018, n. 65, *"Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione"*;
- il Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cybersicurezza, e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («*regolamento sulla cybersicurezza*»)";
- la delibera CIPE (Comitato per la programmazione economica) del 26 novembre 2020, n. 63, che introduce la normativa attuativa della riforma CUP;

- il decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, recante *"Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica"*;
- la legge 30 dicembre 2020, n. 178, recante *"Bilancio di previsione dello Stato per l'anno finanziario 2021 e bilancio pluriennale per il triennio 2021-2023"* e, in particolare, l'articolo 1, comma 1042, ai sensi del quale con uno o più decreti da parte del Ministero dell'Economia e delle Finanze sono stabilite le procedure amministrativo-contabili per la gestione delle risorse di cui ai commi da 1037 a 1050, nonché le modalità di rendicontazione della gestione del Fondo di cui al comma 1037; il comma 1043 del medesimo articolo 1, ai sensi del quale al fine di supportare le attività di gestione monitoraggio, rendicontazione e controllo delle componenti del NGEU, il Ministero dell'Economia e delle Finanze, Dipartimento della Ragioneria generale dello Stato sviluppa e rende disponibile un apposito sistema informatico;
- il Regolamento (UE) 2021/241 del Parlamento Europeo e del Consiglio del 12 febbraio 2021 che istituisce il Dispositivo per la ripresa e la resilienza, come modificato dal Regolamento (UE) 435/23 rispetto all'inserimento di capitoli dedicati al piano REPowerEU nei Piani per la Ripresa e la Resilienza;
- il decreto-legge 31 maggio 2021, n. 77, convertito, con modificazioni, dalla legge 29 luglio 2021, n. 108, recante *"Governance del Piano nazionale di ripresa e resilienza e prime misure di rafforzamento delle strutture amministrative e di accelerazione e snellimento delle procedure"* e, in particolare, l'articolo 8, ai sensi del quale ciascuna Amministrazione centrale titolare di interventi previsti nel PNRR provvede al coordinamento delle relative attività di gestione, nonché al loro monitoraggio, rendicontazione e controllo;
- il decreto-legge 9 giugno 2021, n. 80, convertito, con modificazioni, dalla legge 6 agosto 2021, n. 113, recante *"Misure urgenti per il rafforzamento della capacità amministrativa delle pubbliche amministrazioni funzionale all'attuazione del Piano nazionale di ripresa e resilienza (PNRR) e per l'efficienza della giustizia"*, che definisce percorsi veloci, trasparenti e rigorosi per il reclutamento di profili tecnici e gestionali necessari alle finalità del PNRR, tra cui la cybersicurezza;
- il decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, recante *"Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale"*;
- il Piano Nazionale di Ripresa e Resilienza (di seguito anche "PNRR") – presentato alla Commissione in data 30 giugno 2021 e valutato positivamente con Decisione del Consiglio ECOFIN del 13 luglio 2021, notificata all'Italia dal Segretariato generale del Consiglio con nota LT161/21, del 14 luglio 2021 – e, in particolare, le indicazioni contenute relativamente al raggiungimento di Milestone e Target;
- i principi trasversali previsti dal paragrafo 5.2.1 del PNRR, quali, tra l'altro, il principio del contributo all'obiettivo climatico e digitale (c.d. tagging), il principio di parità di genere, l'obbligo di protezione e valorizzazione dei giovani e del superamento dei divari territoriali;
- gli obblighi di assicurare il conseguimento di target e milestone e degli obiettivi finanziari stabiliti nel PNRR;

- il decreto del Ministro dell'economia e delle finanze del 6 agosto 2021, recante *"Assegnazione delle risorse finanziarie previste per l'attuazione degli interventi del Piano nazionale di ripresa e resilienza (PNRR) e ripartizione di traguardi e obiettivi per scadenze semestrali di rendicontazione"*, che individua il DTD della Presidenza del Consiglio dei ministri quale Amministrazione titolare della Missione 1, Componente 1, Investimento 1.5 recante "Cybersicurezza";
- il Regolamento (UE) 2020/852 del Parlamento europeo e del Consiglio del 18 giugno 2020, relativo all'istituzione di un quadro che favorisce gli investimenti sostenibili e recante modifica del regolamento (UE) 2019/2088, e in particolare l'articolo 17, che definisce gli obiettivi ambientali, tra cui il principio del *"non arrecare un danno significativo"* (DNSH, *"Do no significant harm"*), e la Comunicazione della Commissione UE 2021/C 58/01, recante *"Orientamenti tecnici sull'applicazione del principio non arrecare danno significativo a norma del regolamento sul dispositivo per la ripresa e la resilienza"*;
- il decreto del Presidente del Consiglio dei ministri del 15 settembre 2021, con il quale sono stati individuati gli strumenti per il monitoraggio del PNRR;
- il decreto ministeriale dell'11 ottobre 2021, recante *"Procedure relative alla gestione finanziaria delle risorse previste nell'ambito del PNRR di cui all'articolo 1, comma 1042, della legge 30 dicembre 2020, n. 178"*;
- la circolare del Ministero dell'economia e delle finanze, Dipartimento della Ragioneria generale dello Stato, Servizio centrale per il PNRR, 14 ottobre 2021, n. 21, recante *"Piano Nazionale di Ripresa e Resilienza - Trasmissione delle Istruzioni tecniche per la selezione dei progetti PNRR"*;
- il decreto-legge 6 novembre 2021, n. 152, convertito, con modificazioni, dalla legge 29 dicembre 2021, n. 233, recante *"Disposizioni urgenti per l'attuazione del Piano nazionale di ripresa e resilienza (PNRR) e per la prevenzione delle infiltrazioni mafiose"*;
- la circolare del Ministero dell'economia e delle finanze, Dipartimento della Ragioneria generale dello Stato, 30 dicembre 2021, n. 32, recante *"Piano Nazionale di Ripresa e Resilienza – Guida operativa per il rispetto del principio di non arrecare danno significativo all'ambiente (DNSH)"*, aggiornata con la circolare del 13 ottobre 2022, n. 33 ed errata corrige del 24 ottobre 2022;
- la circolare del Ministero dell'economia e delle finanze, Dipartimento della Ragioneria generale dello Stato, Servizio Centrale per il PNRR, 31 dicembre 2021, n. 33, recante *"Piano Nazionale di Ripresa e Resilienza (PNRR) - Nota di chiarimento sulla Circolare del 14 ottobre 2021, n. 21 - Trasmissione delle Istruzioni Tecniche per la selezione dei progetti PNRR - Addizionalità, finanziamento complementare e obbligo di assenza del c.d. doppio finanziamento"*;
- la circolare del Ministero dell'economia e delle finanze, Dipartimento della Ragioneria generale dello Stato, Servizio Centrale per il PNRR, del 18 gennaio 2022, n. 4, recante *"Piano Nazionale di Ripresa e Resilienza (PNRR) - articolo 1, comma 1, del decreto-legge n. 80 del 2021 - Indicazioni attuative"*;
- la circolare del Ministero dell'economia e delle finanze, Dipartimento della Ragioneria generale dello Stato, Servizio Centrale per il PNRR, 24 gennaio 2022, n. 6, recante *"Piano Nazionale di Ripresa e Resilienza (PNRR) – Servizi di assistenza tecnica per le Amministrazioni titolari di interventi e soggetti attuatori del PNRR"*;

- la circolare del Ministero dell'economia e delle finanze, Dipartimento della Ragioneria generale dello Stato, Servizio Centrale per il PNRR, 10 febbraio 2022, n. 9, recante *"Piano Nazionale di Ripresa e Resilienza (PNRR) - Trasmissione delle Istruzioni tecniche per la redazione dei sistemi di gestione e controllo delle amministrazioni centrali titolari di interventi del PNRR"*;
- la circolare del Ministero dell'economia e delle finanze, Dipartimento della Ragioneria generale dello Stato, Servizio centrale per il PNRR, 29 aprile 2022, n. 21, recante *"Piano nazionale di ripresa e resilienza (PNRR) e Piano nazionale per gli investimenti complementari - Chiarimenti in relazione al riferimento alla disciplina nazionale in materia di contratti pubblici richiamata nei dispositivi attuativi relativi agli interventi PNRR e PNC"*;
- il decreto-legge 30 aprile 2022, n. 36, convertito, con modificazioni, dalla legge 29 giugno 2022, n. 79, recante *"Ulteriori modifiche urgenti per l'attuazione del Piano nazionale di ripresa e resilienza (PNRR)"*;
- la circolare del Ministero dell'economia e delle finanze, Dipartimento della Ragioneria generale dello Stato, Servizio centrale per il PNRR, del 4 luglio 2022, n. 28, recante *"Controllo di regolarità amministrativa e contabile dei rendiconti di contabilità ordinaria e di contabilità speciale. Controllo di regolarità amministrativa e contabile sugli atti di gestione delle risorse del PNRR - prime indicazioni operative"*;
- la circolare del Ministero dell'economia e delle finanze, Dipartimento della Ragioneria generale dello Stato, Servizio Centrale per il PNRR, 26 luglio 2022, n. 29, recante *"Circolare delle procedure finanziarie PNRR"*;
- la circolare del Ministero dell'economia e delle finanze, Dipartimento della Ragioneria generale dello Stato, Servizio Centrale per il PNRR, dell'11 agosto 2022, n. 30, recante *"Circolare sulle procedure di controllo e rendicontazione delle misure PNRR"*, con la quale sono state emanate le *"Linee guida di controllo e rendicontazione delle Misure PNRR di competenza delle Amministrazioni centrali e dei Soggetti Attuatori"*, aggiornate con la circolare del 14 aprile 2023, n. 16 e la circolare 15 settembre 2023, n. 27 recante l'adozione della *"Appendice tematica Rilevazione delle titolarità effettive ex art. 22 par. 2 lett. d) Reg. (UE) 2021/241 e comunicazione alla UIF di operazioni sospette da parte della Pubblica amministrazione ex art. 10, d.lgs. 231/2007"*;
- la circolare del Ministero dell'economia e delle finanze, Dipartimento della Ragioneria generale dello Stato, Servizio Centrale per il PNRR, 2 gennaio 2023, n. 1, recante *"Controllo preventivo di regolarità amministrativa e contabile di cui al decreto legislativo 30 giugno 2011, n. 123. Precisazioni relative anche al controllo degli atti di gestione delle risorse del Piano Nazionale di Ripresa e Resilienza"*;
- la circolare del Ministero dell'economia e delle finanze, Dipartimento della Ragioneria generale dello Stato, Servizio Centrale per il PNRR, 13 marzo 2023, n. 10, recante *"Interventi PNRR. Ulteriori indicazioni operative per il controllo preventivo ed il controllo dei rendiconti delle Contabilità Speciali PNRR aperte presso la Tesoreria dello Stato"*;
- la circolare del Ministero dell'economia e delle finanze, Dipartimento della Ragioneria generale dello Stato, Servizio Centrale per il PNRR, 22 marzo 2023, n. 11, recante *"Registro Integrato dei Controlli PNRR – Sezione controlli milestone e target"*;

- le Linee guida per le Amministrazioni centrali titolari di Interventi PNRR, volte ad assicurare la correttezza delle procedure di attuazione e rendicontazione, la regolarità della spesa e il conseguimento dei target e milestone e di ogni altro adempimento previsto dalla normativa europea e nazionale applicabile al PNRR, a norma dell'articolo 8, comma 3, del decreto-legge 31 maggio 2021, n. 77, convertito, con modificazioni, dalla legge 29 luglio 2021, n. 108;

VISTO, ALTRESÌ, CHE

- l'attuazione del PNRR prevede, per l'attuazione della Missione 1, Componente 1, Investimento 1.5, "Cybersecurity", e la realizzazione degli interventi ad essa connessi, finalizzati all'analisi della postura di sicurezza dei sistemi informativi delle Pubbliche Amministrazioni e alla definizione dei relativi piani di potenziamento delle capacità cyber, l'individuazione delle Amministrazioni centrali in qualità di Soggetti destinatari;
- l'Agenzia per la Cybersicurezza Nazionale è stata individuata quale Soggetto responsabile dell'attuazione dell'Investimento in oggetto, con l'Accordo stipulato, in data 14 dicembre 2021, tra l'Agenzia e il Dipartimento per la trasformazione digitale, ai sensi dell'articolo 5, comma 6, del d.lgs. n. 50/2016, di cui al prot. ACN n. 896 del 15 dicembre 2021, registrato dalla Corte dei Conti il 18 gennaio 2022 al n. 95, e modificato dall'atto aggiuntivo del 14 luglio 2023, registrato dalla Corte dei Conti il 5 settembre 2023 al n. 2425;
- è stata pubblicata la determina n. 25565 del 10/10/2023 di adozione dell'Avviso, approvazione degli atti e nomina del Responsabile del procedimento per l'erogazione di interventi di potenziamento e miglioramento delle capacità cyber degli Organi Costituzionali e di rilevanza Costituzionale, delle Agenzie Fiscali, dei Ministeri, degli Enti di regolazione dell'attività economica, delle Autorità amministrative indipendenti e degli Enti a struttura associativa a valere sul PNRR, Missione 1, Componente 1, Investimento 1.5 "Cybersecurity";
- entro i termini previsti dall'Avviso sono state recepite le istanze di partecipazione contenenti tutte le informazioni al momento disponibili per individuare e quantificare il fabbisogno di supporto dei Soggetti destinatari;
- è stata pubblicata la determina prot. n. 1841 del 19/01/2024 di approvazione della graduatoria finale per l'erogazione di interventi di potenziamento e di miglioramento delle capacità cyber degli Organi Costituzionali e di rilevanza Costituzionale, dei Ministeri, delle Agenzie Fiscali, degli Enti di regolazione dell'attività economica, delle Autorità amministrative indipendenti e degli Enti a struttura associativa a valere sul PNRR, Missione 1, Componente 1, Investimento 1.5 "Cybersecurity";
- il suddetto Avviso prevede l'erogazione da parte dell'Agenzia per la Cybersicurezza Nazionale di interventi di potenziamento e miglioramento delle capacità cyber, avvalendosi di risorse interne e/o propri Fornitori;
- il Contratto stipulato in data 17/11/2021 prot. n. 509, nell'ambito della Convenzione CONSIP AQ 2212 Lotto 1 tra l'Agenzia per la Cybersicurezza Nazionale e il Raggruppamento Temporaneo d'Impresa (RTI) composto da Accenture S.p.A, ESRI Italia S.p.A, Avanade Italy S.r.l, SMC Treviso S.r.l. e-Business Integration Partners S.p.A., prevede la possibilità di erogare i medesimi servizi anche a favore di altre Amministrazioni.

Tutto ciò premesso, visto e considerato, le Parti come sopra individuate convengono e stipulano quanto segue:

Art. 1

Premesse

1. Le premesse sono parte integrante e sostanziale della presente Convenzione unitamente all'allegata Scheda di intervento, i cui contenuti sono stati definiti a seguito degli incontri operativi organizzati per ciascun intervento e sotto-intervento. La stessa potrà essere aggiornata nel tempo, mediante semplice condivisione e accettazione delle Parti, senza necessità di sottoscrivere una nuova Convenzione.

Art. 2

Ruolo delle Parti

1. L'Agenzia per la Cybersicurezza Nazionale (ACN) è individuata quale Soggetto attuatore degli Interventi nell'ambito dell'Investimento 1.5.
2. L'Ispettorato nazionale per la sicurezza nucleare e la radioprotezione è individuato quale Soggetto destinatario finale dell'erogazione degli Interventi nell'ambito dell'Investimento 1.5.

Art. 3

Oggetto

1. La presente Convenzione disciplina i rapporti tra le Parti per l'erogazione dei servizi finalizzati al potenziamento e al miglioramento delle capacità cyber richiesti mediante presentazione dell'Istanza di partecipazione all'Avviso a sportello per l'erogazione di interventi di potenziamento e di miglioramento delle capacità cyber degli Organi costituzionali e di rilevanza Costituzionale, dei Ministeri, delle Agenzie Fiscali, degli Enti di regolazione dell'attività economica, delle Autorità amministrative indipendenti e degli Enti a struttura associativa, nell'ambito della realizzazione degli obiettivi previsti dal PNRR, Missione 1, Componente 1, Investimento 1.5 "Cybersecurity", e dettagliati nella Scheda di Intervento allegata.
2. La presente Convenzione definisce, inoltre, gli obblighi delle Parti e le procedure di rendicontazione.

Art. 4

Termini di attuazione del progetto e risorse finanziarie assegnate

1. Le attività, indicate nella Scheda di intervento allegata, dovranno essere avviate secondo i tempi concordati nei singoli Verbali di avvio degli interventi tra il Soggetto attuatore e il Soggetto destinatario.
2. Il servizio erogato dovrà concludersi entro la data indicata nella citata Scheda di intervento e nel rispetto delle tempistiche previste dal PNRR; al fine di attestare la conclusione degli interventi, per poi procedere alla quantificazione dei costi reali, il Soggetto attuatore predisporrà il Verbale di

chiusura degli stessi interventi in linea con quanto previsto dall'Avviso e nel rispetto di quanto indicato in fase di attuazione.

3. Per l'erogazione dei servizi, l'importo massimo ammesso a finanziamento è pari a € 637.500,00 (seicentotrentasettemilacinquecento/00), ripartito per ciascun servizio richiesto così come indicato nella Scheda di intervento.

Art. 5

Obblighi del Soggetto destinatario

1. Con la sottoscrizione della presente Convenzione, il Soggetto destinatario si obbliga a:

- fornire la necessaria collaborazione per lo svolgimento di tutte le attività previste nella Convenzione, nei termini ivi indicati e con le modalità di cui alla Scheda di Intervento;
- collaborare, preliminarmente, all'ultimazione dell'attività obbligatoria "1.1 Analisi di dettaglio delle procedure, processi e organizzazione delle capacità cyber" per poter procedere alle successive attività pianificate nella scheda di intervento allegata alla Convezione;
- collaborare all'ultimazione degli interventi finanziati e previsti nella Scheda di Intervento;
- collaborare con il Soggetto attuatore per assicurare il rispetto di tutte le disposizioni previste dalla normativa europea e nazionale, con particolare riferimento a quanto previsto dal Regolamento (UE) 2021/241 e dal decreto-legge del 31 maggio 2021, n. 77, recante *"Governance del Piano nazionale di ripresa e resilienza e prime misure di rafforzamento delle strutture amministrative e di accelerazione e snellimento delle procedure"*, convertito, con modificazioni, dalla legge 29 luglio 2021, n. 108;
- collaborare con il Soggetto attuatore per garantire il rispetto del principio di *"non arrecare un danno significativo"* agli obiettivi ambientali ai sensi dell'articolo 17 del Regolamento (UE) 2020/852 (DNSH) e garantire la coerenza con il PNRR valutato positivamente con Decisione del Consiglio ECOFIN del 13 luglio 2021;
- collaborare con il Soggetto attuatore per rispettare le condizioni prescrittive necessarie all'assolvimento del principio del contributo all'obiettivo climatico e digitale (cd. tagging);
- collaborare con il Soggetto attuatore nell'assicurare l'adozione di misure adeguate volte a rispettare il principio di sana gestione finanziaria secondo quanto disciplinato dal Regolamento finanziario (UE, Euratom) 2018/1046 e dall'articolo 22 del Regolamento (UE) 2021/241, in particolare in materia di prevenzione, identificazione e rettifica dei conflitti di interessi, delle frodi, della corruzione e di recupero e restituzione dei fondi che sono stati indebitamente assegnati, nonché di garantire l'assenza del c.d. doppio finanziamento ai sensi dell'articolo 9 del Regolamento (UE) 2021/241;
- collaborare con il Soggetto attuatore per rispettare le norme europee e nazionali applicabili in ambito di tutela dei soggetti diversamente abili;
- collaborare con il Soggetto attuatore per rispettare i principi di parità di trattamento, non discriminazione, trasparenza, proporzionalità e pubblicità;

- collaborare con il Soggetto attuatore per individuare eventuali fattori che possano determinare ritardi che incidano in maniera considerevole sulla tempistica attuativa e di spesa, definita nel cronoprogramma, relazionando all'Agenzia sugli stessi;
- collaborare con il Soggetto attuatore per mitigare e gestire i rischi connessi al progetto nonché per porre in essere azioni mirate connesse all'andamento gestionale ed alle caratteristiche tecniche;
- fornire supporto per la rendicontazione degli indicatori di realizzazione associati al progetto, in riferimento al contributo al perseguimento dei target e milestone del PNRR;
- collaborare con il Soggetto attuatore per garantire la correttezza, l'affidabilità e la congruenza dei dati di monitoraggio di propria competenza con il tracciato informativo previsto per l'alimentazione del sistema informativo PNRR (ReGiS) dei dati di monitoraggio finanziario, fisico e procedurale, e di quelli che comprovano il conseguimento degli obiettivi dell'intervento quantificati in base agli stessi indicatori adottati per i milestone e i target della misura e assicurarne l'inserimento nel sistema informativo utilizzato dall'Amministrazione responsabile dei dati di monitoraggio sull'avanzamento procedurale, fisico e finanziario del progetto, ex articolo 22, comma 2, lettera d), del Regolamento (UE) 2021/241, nonché le informazioni a comprova del conseguimento delle milestone e dei target associati all'intervento, ivi inclusa la documentazione probatoria e tenendo conto delle indicazioni che verranno fornite dall'Amministrazione responsabile;
- rispettare gli adempienti in materia di trasparenza amministrativa ex del decreto legislativo 25 maggio 2016, n. 97, e gli obblighi in materia di comunicazione e informazione previsti dall'articolo 34 del Regolamento (UE) 2021/241;
- rendere nota l'origine del finanziamento e garantirne visibilità riportando in tutta la documentazione di progetto il logo dell'Unione Europea e utilizzando la dicitura "Finanziato dall'Unione Europea – Next Generation UE – PNRR M1C1 – Investimento 1.5";
- conservare – nel rispetto di quanto previsto dal decreto legislativo 82/2005 e dall'articolo 9, comma 4 del decreto-legge 31 maggio 2021, n. 77, convertito, con modificazioni, dalla legge 29 luglio 2021, n. 108 – la documentazione progettuale, inclusa quella relativa ai target realizzati, per assicurare la completa tracciabilità delle operazioni che, nelle diverse fasi di controllo e verifica previste dal sistema di gestione e controllo del PNRR, deve essere messa prontamente a disposizione su richiesta dell'Agenzia per la Cybersicurezza Nazionale, dell'Amministrazione centrale titolare dell'intervento, del Servizio centrale per il PNRR del MEF, dell'Unità di Audit, della Commissione europea, dell'Ufficio europeo per la lotta antifrode, della Corte dei Conti europea (ECA), della Procura europea (EPPO) e delle competenti Autorità giudiziarie nazionali;
- autorizzare la Commissione, l'Ufficio europeo per la lotta antifrode, la Corte dei conti e l'EPPO a esercitare i diritti di cui all'articolo 129, paragrafo 1, del Regolamento finanziario (UE; EURATOM) 1046/2018;
- partecipare, ove richiesto, alle riunioni convocate dall'Agenzia;
- garantire una tempestiva, diretta, informazione agli organi preposti, tenendo informato il Soggetto attuatore sull'eventuale avvio e andamento di procedimenti di carattere giudiziario,

civile, penale o amministrativo che dovessero interessare le attività oggetto del progetto finanziato;

- comunicare le irregolarità o le frodi eventualmente riscontrate a seguito delle verifiche di competenza e adottare le misure necessarie, nel rispetto delle procedure adottate dall'Agenzia, in linea con quanto indicato dall'articolo 22 del Regolamento (EU) 2021/241;
- garantire la massima collaborazione in occasione di verifiche e controlli richiesti dall'Agenzia per la Cybersicurezza Nazionale, dal Servizio centrale per il PNRR, dall'Unità di audit, della Commissione europea, dell'Ufficio europeo per la lotta antifrode, della Corte dei conti europea (ECA), della Procura europea (EPPO) e delle competenti Autorità giudiziarie nazionali, nonché eventualmente dalle forze di polizia nazionali.

Art. 6

Obblighi del Soggetto attuatore

1. Con la sottoscrizione della presente Convenzione, l'Agenzia per la Cybersicurezza Nazionale si obbliga a:

- assicurare il rispetto di tutte le disposizioni previste dalla normativa europea e nazionale, con particolare riferimento al disposto del Regolamento (UE) 2021/241 e del decreto-legge n. 77 del 31 maggio 2021, convertito, con modificazioni, dalla legge 29 luglio 2021, n. 108;
- assicurare l'adozione di misure adeguate volte a rispettare il principio di sana gestione finanziaria secondo quanto disciplinato dal Regolamento finanziario (UE, Euratom) 2018/1046 e dall'articolo 22 del Regolamento (UE) 2021/241, in particolare in materia di prevenzione, identificazione e rettifica dei conflitti di interessi, delle frodi, della corruzione e di recupero e restituzione dei fondi che sono stati indebitamente assegnati, nonché di garantire l'assenza del c.d. doppio finanziamento ai sensi dell'articolo 9 del Regolamento (UE) 2021/241;
- rispettare, ove applicabile, il principio di *"non arrecare un danno significativo"* agli obiettivi ambientali ai sensi dell'articolo 17 del Regolamento (UE) 2020/852 (DNSH) e garantire la coerenza con il PNRR valutato positivamente con Decisione del Consiglio ECOFIN del 13 luglio 2021;
- rispettare, ove applicabili, le condizioni prescrittive necessarie all'assolvimento del principio del contributo all'obiettivo climatico e digitale (cd. tagging);
- rispettare la normativa applicabile in tema di trattamento dei dati personali e, in particolare, il Regolamento (UE) 2016/679 (GDPR);
- rispettare, ove applicabili, gli ulteriori principi trasversali previsti per il PNRR dalla normativa nazionale ed europea, con particolare riferimento alla protezione e valorizzazione dei giovani e del superamento dei divari territoriali;
- introdurre nella fase di esecuzione, ove applicabili, misure a sostegno della partecipazione di donne e giovani, anche in coerenza con quanto previsto dall'articolo 47, del decreto-legge 31 maggio 2021, n. 77 (c.d. decreto Semplificazioni), convertito in legge 29 luglio 2021, n. 108;
- rispettare le norme europee e nazionali applicabili in ambito di tutela dei soggetti diversamente abili;

- rispettare i principi di parità di trattamento, non discriminazione, trasparenza, proporzionalità e pubblicità;
- garantire il rispetto del principio di parità di genere in relazione agli articoli 2, 3, paragrafo 3, del TUE, 8, 10, 19 e 157 del TFUE, e 21 e 23 della Carta dei diritti fondamentali dell'Unione europea;
- dare piena attuazione agli interventi così come illustrati nella Scheda Intervento ed avviare tempestivamente le attività per non incorrere in ritardi attuativi;
- concludere gli interventi nei modi e nei tempi previsti, e provvedere alla comunicazione tempestiva all' Amministrazione centrale titolare dell'intervento delle date di avvio degli stessi tramite Verbale di avvio degli interventi;
- garantire la correttezza, l'affidabilità e la congruenza al tracciato del sistema informativo unitario per il PNRR di cui all'articolo 1, comma 1043, della legge n. 178/2020 (ReGiS) dei dati di monitoraggio finanziario, fisico e procedurale, e di quelli che comprovano il conseguimento degli obiettivi dell'intervento quantificati in base agli stessi indicatori adottati per milestone e target della misura e assicurarne l'inserimento nel sistema informativo e gestionale adottato dalla Amministrazione centrale titolare dell'intervento responsabile nel rispetto delle indicazioni che saranno fornite dalla stessa Amministrazione;
- adottare un'apposita codificazione contabile e informatizzata per tutte le transazioni relative al progetto al fine di assicurare la tracciabilità dell'utilizzo delle risorse del PNRR;
- effettuare i controlli di gestione e amministrativo-contabili previsti dalla legislazione nazionale applicabile per garantire la regolarità delle procedure e delle spese sostenute prima di rendicontarle alla Amministrazione centrale titolare dell'intervento, nonché la riferibilità delle spese al progetto ammesso al finanziamento sul PNRR;
- fornire tutte le informazioni richieste relativamente alle procedure e alle verifiche in relazione alle spese rendicontate conformemente alle procedure e agli strumenti definiti nella manualistica adottata dall'Amministrazione centrale titolare dell'intervento;
- assicurare la completa tracciabilità dei flussi finanziari come previsto dall'articolo 3, della legge 3 agosto 2016, n. 136, e prevedere una modalità di gestione finanziaria che sia conforme alle disposizioni del Regolamento finanziario (UE, Euratom) 2018/1046 e dell'articolo 22 del Regolamento (UE) 2021/241, in materia di prevenzione di sana gestione finanziaria, assenza di conflitti di interessi, di frodi e corruzione;
- rilevare e imputare nel sistema informativo i dati di monitoraggio sull'avanzamento procedurale, fisico e finanziario del progetto, *ex* articolo 22, comma 2, lettera d), del Regolamento (UE) 2021/241, nonché le informazioni a comprova del conseguimento delle milestone e dei target associati all'intervento, ivi inclusa la documentazione probatoria;
- garantire la correttezza, l'affidabilità e la congruenza dei dati di monitoraggio di cui sopra;
- rispettare gli adempienti in materia di trasparenza amministrativa *ex* decreto legislativo 25 maggio 2016, n. 97 e gli obblighi in materia di comunicazione e informazione previsti dall'articolo 34 del Regolamento (UE) 2021/241;

- rendere nota l'origine del finanziamento e garantirne visibilità utilizzando in tutta la documentazione di progetto la dicitura "Finanziato dall'Unione europea – Next Generation UE – PNRR M1C1 – Investimento 1.5" e riportando il logo dell'Unione europea in ogni intestazione di pagina;
- alimentare, ove richiesto, i dati in Sistema di Gestione Progetti (SGP) relativamente a tutti gli aspetti procedurali, fisici e finanziari secondo le procedure ed i manuali che saranno forniti all'atto della sottoscrizione della Convenzione di accettazione del contributo;
- conservare - nel rispetto di quanto previsto dal decreto legislativo 82/2005 e all'articolo 9, comma 4, del decreto-legge n. 77 del 31 maggio 2021 - la documentazione progettuale per assicurare la completa tracciabilità delle operazioni che, nelle diverse fasi di controllo e verifica previste dal sistema di gestione e controllo del PNRR, deve essere messa prontamente a disposizione su richiesta dell'Agenza per la Cybersicurezza Nazionale, dell'Amministrazione centrale titolare dell'intervento, del Servizio centrale per il PNRR del MEF, dell'Unità di Audit, della Commissione europea, dell'Ufficio europeo per la lotta antifrode, della Corte dei conti europea (ECA), della Procura europea (EPPO) e delle competenti Autorità giudiziarie nazionali;
- autorizzare la Commissione, l'Ufficio europeo per la lotta antifrode, la Corte dei conti e l'EPPO a esercitare i diritti di cui all'articolo 129, paragrafo 1, del Regolamento finanziario (UE; EURATOM) 1046/2018;
- garantire, anche attraverso la trasmissione di relazioni periodiche sullo stato di avanzamento del progetto, che l'Amministrazione centrale titolare dell'intervento riceva tutte le informazioni necessarie, relative alle linee di attività per l'elaborazione delle relazioni annuali di cui all'articolo 31 del Regolamento (UE) n. 2021/241, nonché qualsiasi altra informazione eventualmente richiesta;
- contribuire al raggiungimento dei milestone e target associati alla Misura e fornire, su richiesta dell'Amministrazione centrale titolare dell'intervento, le informazioni necessarie per la predisposizione delle dichiarazioni sul conseguimento dei target e milestone e delle relazioni e documenti sull'attuazione dei progetti;
- garantire una tempestiva, diretta, informazione agli organi preposti, tenendo informata la Amministrazione centrale titolare dell'intervento sull'eventuale avvio e andamento di procedimenti di carattere giudiziario, civile, penale o amministrativo che dovessero interessare le attività oggetto del progetto finanziato;
- comunicare le irregolarità o le frodi eventualmente riscontrate a seguito delle verifiche di competenza e adottare le misure necessarie, nel rispetto delle procedure adottate dalla Amministrazione centrale titolare dell'intervento, in linea con quanto indicato dall'articolo 22 del Regolamento (EU) 2021/2041;
- garantire la massima collaborazione in occasione di verifiche e controlli richiesti dall' Amministrazione centrale titolare dell'intervento, dal Servizio centrale per il PNRR, dall'Unità di Audit, dalla Commissione europea, dall'Ufficio europeo per la lotta antifrode, dalla Corte dei Conti europea (ECA), della Procura europea (EPPO) e dalle competenti Autorità giudiziarie nazionali, nonché eventualmente delle Forze di polizia nazionali;

- assolvere ad ogni altro onere e adempimento previsto a dalla normativa europea in vigore, per tutta la durata della presente Convenzione.

Art. 7

Disimpegno delle risorse

1. L'eventuale disimpegno delle risorse del Piano, previsto dall'articolo 24 del Regolamento 2021/241 e dall'articolo 8 della legge n. 77 del 2021, comporta la riduzione o revoca delle risorse destinate a finanziare i progetti che non hanno raggiunto gli obiettivi previsti, nel rispetto di quanto previsto dall'Avviso.
2. Il Soggetto destinatario è obbligato a fornire tempestivamente ogni informazione in merito ad errori od omissioni che possano dar luogo a riduzione o revoca del contributo.

Art. 8

Risoluzione di controversie

1. La presente Convenzione è regolata dalla legge italiana. Qualsiasi controversia, in merito all'interpretazione, esecuzione, validità o efficacia della presente Convenzione, è di competenza esclusiva del Foro di Roma.

Art. 9

Risoluzione per inadempimento

1. L'Agenzia per la Cybersicurezza Nazionale potrà avvalersi della facoltà di risolvere la presente Convenzione qualora il Soggetto destinatario non rispetti gli obblighi imposti a suo carico previsti dall'articolo 5 della presente Convenzione e, comunque, pregiudichi l'assolvimento da parte della stessa Agenzia degli obblighi imposti dalla normativa europea.

Art. 10

Diritto di recesso

1. L'Agenzia per la Cybersicurezza Nazionale potrà recedere in qualunque momento dagli impegni assunti con la presente Convenzione nei confronti del Soggetto destinatario qualora, a proprio giudizio, nel corso di svolgimento delle attività, intervengano fatti o provvedimenti che modifichino la situazione esistente all'atto della stipula della presente Convenzione o ne rendano impossibile o inopportuna la conduzione a termine.

Art. 11

Cause di risoluzione per inadempimento

1. Nel caso di inadempimento e violazione degli obblighi posti in capo al Soggetto destinatario, può essere disposta la sospensione del finanziamento e dei servizi. Nello specifico, sarà valutata la revoca totale o parziale del finanziamento nei seguenti casi di inadempimento e violazione da parte del Soggetto destinatario:

- parziale o mancato conseguimento di target, milestone e degli obiettivi previsti, anche di natura finanziaria, nei tempi assegnati, al fine di salvaguardare il raggiungimento di target e milestone intermedi e finali associati all'investimento;

- sospetta violazione dei principi generali di DNSH e/o del principio del tagging e/o accertamento della violazione;
- gravi violazioni di leggi e regolamenti e violazione e/o inadempienza agli obblighi di cui all'Avviso;
- mancata collaborazione con l'Agenzia nella fase di rendicontazione delle spese.

2. In caso di revoca, parziale o totale, il Soggetto destinatario è tenuto alla restituzione delle somme impiegate per l'erogazione dei servizi eventualmente ricevuti, a cui saranno applicati gli interessi di mora ove ne ricorrano i presupposti.
3. Il Soggetto destinatario potrà rinunciare all'erogazione del contributo; in caso di rinuncia è tenuto alla restituzione delle somme impiegate per l'erogazione dei servizi eventualmente ricevuti, a cui saranno applicati gli interessi di mora ove ne ricorrano i presupposti.

Art. 12

Comunicazioni e scambio di informazioni

1. Ai fini della digitalizzazione dell'intero ciclo di vita dell'intervento, tutte le comunicazioni con l'Agenzia per la Cybersicurezza Nazionale devono avvenire per posta elettronica istituzionale o posta elettronica certificata, ai sensi del decreto legislativo n. 82/2005.
2. Nello specifico, si stabiliscono le seguenti modalità di invio telematico:

- Convenzione: obbligatorio l'invio all'indirizzo di posta elettronica certificata (PEC) pnrr@pec.acn.gov.it, con l'indicazione nell'oggetto "Avviso 7/2023 – Convenzione – *nome Soggetto destinatario*, del documento firmato digitalmente da entrambe le parti;
- comunicazioni in autocertificazione ai sensi del d.P.R. n. 445/2000: invio a mezzo posta elettronica istituzionale con allegata fotocopia del documento del dichiarante;
- comunicazioni ordinarie: invio a mezzo posta elettronica istituzionale.

Art. 13

Obblighi di informazione e pubblicità

1. È compito del Soggetto destinatario dare adeguata pubblicità del finanziamento europeo, anche ai destinatari dell'intervento stesso, nelle modalità di cui al PNRR previsti dall'articolo 34 del Regolamento (UE) 2021/241;
2. Le iniziative di pubblicità e comunicazione afferenti alla realizzazione degli interventi dovranno essere comunicate, con congruo anticipo, all'Agenzia per la Cybersicurezza Nazionale, che potrà indicare tempi e modalità di attuazione, vincolanti per il Soggetto destinatario.

Art. 14

Conflitto d'interessi e incompatibilità

1. Il Soggetto destinatario si impegna ad adottare ogni necessaria misura per prevenire ovvero eliminare ogni rischio di conflitto di interesse o incompatibilità che possa incidere, anche indirettamente, sull'imparzialità e l'obiettività di attuazione della presente Convenzione (i.e. interessi economici, affinità politiche o territoriali, ragioni personali o familiari, interessi condivisi ecc.).
2. Ogni situazione che costituisce o può costituire un conflitto d'interesse o una condizione di incompatibilità durante l'esecuzione delle attività deve essere immediatamente comunicata all'Agenzia per la Cybersicurezza Nazionale. Il Soggetto destinatario deve procedere senza alcun indugio alla rimozione delle situazioni di conflitto.
3. L'Agenzia per la Cybersicurezza Nazionale si riserva il diritto di verificare che le misure prese siano appropriate e di richiedere, se necessario, ulteriori azioni correttive. Nel caso la situazione di conflitto dovesse permanere, l'Agenzia per la Cybersicurezza Nazionale applicherà le sanzioni previste nell'Avviso al paragrafo n. 8.3 "Meccanismi sanzionatori e rinuncia al contributo".

Art. 15

Disposizioni Finali

1. Per quanto non previsto dalla presente Convenzione si rinvia alle norme europee e nazionali di riferimento.

Art. 16

Modifiche ed Integrazioni

1. Ogni modifica o integrazione ritenuta opportuna o necessaria, anche se connessa all'entrata in vigore di nuove norme disciplinanti la materia, per essere valida ed efficace deve risultare da atto debitamente firmato dalle Parti.
2. Eventuali modifiche alle modalità operative che non determinino variazioni sostanziali del presente Accordo possono essere apportate con consenso unanime delle Parti tramite PEC e/o PEO, nelle quali le Parti determineranno la data di decorrenza dell'efficacia delle previsioni concordate.
3. Le eventuali modifiche e/o integrazioni alla presente Convenzione dovranno essere previamente concordate per iscritto tra le Parti.

Art. 17

Efficacia e durata

1. La presente Convenzione decorre dalla data di sottoscrizione della stessa ed è efficace fino all'esatto ed integrale adempimento di tutte le obbligazioni contrattuali qui disciplinate e, comunque, fino alla data di chiusura del progetto nel rispetto delle tempistiche previste dal PNRR. Più nello specifico, quindi, fino alla chiusura delle attività di rendicontazione, fermo restando il rispetto degli obblighi di cui all'art. 5 "Obblighi del Soggetto destinatario".

Roma, __/__/_____

Per il Soggetto attuatore

Il Direttore Generale

Bruno Frattasi

(*in formato digitale*)

Per il Soggetto destinatario

Qualifica

Nome e Cognome

(*in formato digitale*)

Le Parti, ai sensi e per gli effetti degli artt. 1341 e 1342 c.c., dichiarano di approvare specificamente gli articoli 9, 10 e 11 della presente Convenzione.

Per il Soggetto attuatore

Il Direttore Generale

Bruno Frattasi

(*in formato digitale*)

Per il Soggetto destinatario

Qualifica

Nome e Cognome

(*in formato digitale*)

Art. 1

AGENZIA PER LA CYBERSICUREZZA NAZIONALE
PNRR Missione 1 - Componente 1 - Investimento 1.5 "Cybersecurity"

SCHEDA DI INTERVENTO

ANAGRAFICA	
ID	18_WP9_A7_ISPA
Referente del Soggetto richiedente	Maurizio Pimpo
Denominazione del Soggetto richiedente	Ispettorato Nazionale per la Sicurezza Nucleare e la Radioprotezione
Sede dell'intervento	Roma
Data inizio e fine prevista	01/03/2024 - 29/11/2024

INTERVENTI FINANZIATI			
Sottointervento	Descrizione sintetica del Sotto-intervento	Massimale sottointervento	Tipologia intervento
1.1 Analisi di dettaglio delle procedure, processi e organizzazione delle capacità cyber	Valutazione del punto di vista organizzativo e dei processi della maturità cyber del Soggetto destinatario, identificando i punti di miglioramento e definendo una strategia evolutiva volta a incrementare il relativo livello di maturità	130.000,00 €	1. Analisi della postura di sicurezza e piano di potenziamento
1.2 Analisi di vulnerabilità del rischio eseguite sui principali asset del Soggetto destinatario	Valutazione del rischio cyber sui principali asset IT critici del Soggetto destinatario (qualora non sia disponibile un catalogo di servizi consolidato presso il Soggetto Destinatario, tali asset IT saranno individuati mediante il sotto- intervento #1.3)	150.000,00 €	1. Analisi della postura di sicurezza e piano di potenziamento
2.1 Definizione e/o potenziamento del processo a supporto della continuità operativa	Valutazione del processo a supporto della continuità operativa in essere presso il contesto di riferimento, definizione di un piano di potenziamento strategico e conseguente elaborazione e/o ottimizzazione della relativa policy a supporto. Conduzione di attività di Business Impact Analysis (BIA) su un sotto-insieme di servizi critici e definizione di strategie di continuità operativa da implementare al fine di garantire la continuità di tali servizi. Qualora il Soggetto destinatario non abbia definito un catalogo servizi, il sotto-insieme di servizi critici oggetto di BIA è individuato tramite analisi, interviste ed	100.000,00 €	2. Miglioramento dei processi e dell'organizzazione di gestione della cybersecurity
2.2 Definizione e/o potenziamento del processo di gestione delle vulnerabilità e di sviluppo sicuro del codice	Valutazione dei processi di gestione delle vulnerabilità e di sviluppo sicuro del codice eventualmente in essere presso il contesto di riferimento, definizione di un piano di potenziamento strategico e conseguente elaborazione e/o ottimizzazione dei relativi manuali operativi/procedure a supporto	200.000,00 €	2. Miglioramento dei processi e dell'organizzazione di gestione della cybersecurity
3.1 Servizi di cybersecurity awareness	Erogazione di sessioni informative su tematiche di cybersecurity a beneficio del personale dei Soggetti destinatari, attraverso lo sviluppo e la condivisione di materiale interattivo	7.500,00 €	3. Miglioramento delle competenze delle persone
		537.500,00 €	

Allegato ART-1

1. Analisi della postura di sicurezza e piano di potenziamento	1.1 Analisi di dettaglio delle procedure, processi e organizzazione delle capacità cyber	1. Analisi della postura di sicurezza e piano di potenziamento	Valutazione del piano di cyber organizzativo e dei processi della sicurezza cyber del Soggetto destinatario, identificando i punti di
1. Analisi della postura di sicurezza e piano di potenziamento	1.2 Analisi delle capacità dei sistemi e strumenti di sicurezza in essere	1. Analisi della postura di sicurezza e piano di potenziamento	Valutazione tecnologica della sicurezza cyber del Soggetto destinatario, identificando i punti di miglioramento e definendo una strategia evolutiva volta a incrementare il relativo livello di sicurezza
1. Analisi della postura di sicurezza e piano di potenziamento	1.3 Analisi di valutazione del rischio cyber sui principali asset del Soggetto destinatario	1. Analisi della postura di sicurezza e piano di potenziamento	Valutazione del rischio cyber sui principali asset IT critici del Soggetto destinatario (qualora non sia disponibile un catalogo di servizi consultabile presso il Soggetto Destinatario, tali asset IT vengono individuati mentre il sotto intervento #1.1)
2. Miglioramento dei processi e dell'organizzazione di gestione della cybersecurity	2.1 Definizione e/o potenziamento del processo di gestione degli incidenti di natura cyber e di backup e restore	2. Miglioramento nei processi e dell'organizzazione di gestione della cybersecurity	Valutazione dei processi di gestione degli incidenti di natura cyber e di backup e restore eventualmente in essere presso il contesto di riferimento, definizione di un piano di potenziamento strategico e conseguente elaborazione e/o armonizzazione delle relative procedure e supporto
2. Miglioramento dei processi e dell'organizzazione di gestione della cybersecurity	2.2 Definizione e/o potenziamento del processo di security by design	2. Miglioramento dei processi e dell'organizzazione di gestione della cybersecurity	Valutazione del processo e della metodologia di security by design eventualmente in essere presso il contesto di riferimento, definizione di un piano di potenziamento tecnologico e conseguente elaborazione e/o armonizzazione della relativa procedura e supporto
2. Miglioramento dei processi e dell'organizzazione di gestione della cybersecurity	2.3 Definizione e/o potenziamento dei processi a supporto della continuità operativa	2. Miglioramento dei processi e dell'organizzazione di gestione della cybersecurity	Valutazione del processo e supporto della continuità operativa e ausiliari presso il contesto di riferimento, definizione di un piano di potenziamento strategico e conseguente elaborazione e/o armonizzazione della relativa politica a supporto. Conduzione di analisi di Business Impact Analysis (BIA) su un sotto-insieme di servizi critici e definizione di strategie di continuità operativa da implementare al fine di garantire la continuità di tali servizi. (Qualora il Soggetto destinatario non abbia redatto un catalogo servizi, il sotto-insieme di servizi utili oggetto di BIA è individuato tramite sotto intervento #1.1)
2. Miglioramento dei processi e dell'organizzazione di gestione della cybersecurity	2.4 Definizione e/o potenziamento del processo di gestione delle vulnerabilità e di sviluppo sicuro del codice	2. Miglioramento del processo e dell'organizzazione di gestione della cybersecurity	Valutazione dei processi di gestione delle vulnerabilità e di sviluppo sicuro del codice eventualmente in essere presso il contesto di riferimento, definizione di un piano di potenziamento strategico e conseguente elaborazione e/o armonizzazione dei relativi manuali operativi/procedure e supporto
2. Miglioramento dei processi e dell'organizzazione di gestione della cybersecurity	2.5 Definizione e/o potenziamento del processo di gestione delle identità digitali e degli accessi ai sistemi informativi	2. Miglioramento dei processi e dell'organizzazione di gestione della cybersecurity	Valutazione del processo di gestione delle identità digitali e degli accessi ai sistemi informativi eventualmente in essere presso il contesto di riferimento, definizione di un piano di potenziamento strategico e conseguente elaborazione e/o armonizzazione della relativa politica/procedura a supporto
2. Miglioramento dei processi e dell'organizzazione di gestione della cybersecurity	2.6 Supporto in ambito Network Security: analisi della rete e piano di riorganizzazione	2. Miglioramento dei processi e dell'organizzazione di gestione della cybersecurity	Valutazione della zone di sicurezza della rete del Soggetto destinatario approfondendo e anche eventualmente i sistemi emersi in
2. Miglioramento dei processi e dell'organizzazione di gestione della cybersecurity	2.7 Revisione e potenziamento del framework documentale (politiche/procedure) di sicurezza sulla base delle evidenze emerse dalle attività di analisi	2. Miglioramento dei processi e dell'organizzazione di gestione della cybersecurity	Revisione del framework documentale di sicurezza attualmente definito presso il contesto di riferimento, identificazione ed elaborazione – anche in base alle evidenze emerse dal sotto-intervento #1.1 "Analisi della postura di sicurezza" – delle politiche/processi rilevanti per incrementare la postura di sicurezza del Soggetto destinatario
2. Miglioramento dei processi e dell'organizzazione di gestione della cybersecurity	2.8 Definizione di un modello di CSIRT/SOC	2. Miglioramento dei processi e dell'organizzazione di gestione della cybersecurity	Identificazione dell'attuale organizzazione preposta al controllo e al governo della sicurezza (sulla prevenzione delle minacce cyber fino alla gestione degli incidenti di sicurezza) e predisposizione di un modello CSIRT/SOC (ex. confluenza di riferimento, servizi da erogare, ecc.) a partire dal contesto in essere e sulla base delle buone pratiche di settore
2. Miglioramento dei processi e dell'organizzazione di gestione della cybersecurity	2.9 Revisione e potenziamento dell'organizzazione della cybersicurezza e disegno dei relativi processi	2. Miglioramento dei processi e dell'organizzazione di gestione della cybersecurity	Revisione e potenziamento dell'attuale organizzazione di cybersecurity del Soggetto destinatario, identificando ruoli, responsabilità e processi a supporto della sicurezza informatica al fine di individuare potenziali punti evolutivi e definire/potenziare il modello di Information Security Governance
3. Miglioramento della consapevolezza della persona	3.1 Servizi di cybersecurity awareness	3. Miglioramento della consapevolezza della persona	Erogazione di sessioni informative su tematiche di cybersecurity a beneficio del personale del Soggetti destinatari, attraverso lo sviluppo e la condivisione di contenuti interattivi