MINISTERO del LAVORO
e delle POLITICHE SOCIALI

IL DIRETTORE GENERALE

VISTO il R.D. 18 novembre 1923, n. 2440, concernente l'amministrazione del patrimonio e la contabilità generale dello Stato e il relativo Regolamento approvato con R.D. 23 maggio 1924, n. 827;

VISTO il D.lgs. 30 marzo 2001, n. 165, recante "Norme generali sull'ordinamento alle dipendenze delle Amministrazioni pubbliche";

VISTO il D.P.R. 15 marzo 2017, n. 57, recante il "Regolamento di organizzazione del Ministero del lavoro e delle politiche sociali", pubblicato sulla G.U. n. 103 del 05 maggio 2017 - Serie Generale, in vigore dal 20 maggio 2017;

VISTO il D.P.C.M. 24 giugno 2021, n. 140, recante modifiche al regolamento di organizzazione del Ministero del lavoro e delle politiche sociali, pubblicato sulla G.U. n. 241 dell'8 ottobre 2021 - Serie Generale, in vigore dal 23 ottobre 2021;

VISTO il Decreto del Ministro del lavoro e delle politiche sociali 25 gennaio 2022, recante l'"Individuazione delle unità organizzative di livello dirigenziale non generale nell'ambito del Segretariato generale e delle Direzioni generali", registrato dalla Corte dei Conti in data 14 febbraio 2022 al n. 299 e pubblicato sulla G.U. n. 60 del 12 marzo 2022 - Serie Generale;

VISTO il Decreto del Ministro dell'economia e delle finanze del 30 dicembre 2022, pubblicato sulla G.U. n. 304 del 30 dicembre 2022 - Suppl. Ordinario n. 44, concernente la "Ripartizione in capitoli delle Unità di voto parlamentare relative al bilancio di previsione dello Stato per l'anno finanziario 2023 e per il triennio 2023 - 2025" e, in particolare, la Tabella 4, riguardante il bilancio di previsione del Ministero del lavoro e delle politiche sociali;

VISTO il Decreto del Ministro del lavoro e delle politiche sociali n. 12 dell'8 febbraio 2023, registrato dall'Ufficio Centrale del Bilancio al n. 77 del 22 febbraio 2023, di ripartizione e assegnazione delle risorse umane e finanziarie per l'anno 2023 ai Dirigenti degli Uffici dirigenziali di livello generale, titolari dei centri di responsabilità amministrativa;

VISTO il D.lgs. 31 marzo 2023, n. 36, recante il "Codice dei Contratti Pubblici" e l'allegato II.1;

VISTO che l'art. 37 del D.lgs. n. 36/2023 ha introdotto una programmazione triennale anche per gli acquisti di beni e servizi;

CONSIDERATO che, ai sensi dell'art. 225 comma 2 D.lgs. 36/2023 "*Disposizioni transitorie e di coordinamento*", le disposizioni di cui all'art. 37 acquistano efficacia a decorrere dal 1° gennaio 2024 e che, pertanto, si procede ad approvare il programma biennale degli acquisti ai sensi dell'articolo 21 del d. lgs. 50/2016;

VISTO il Decreto Direttoriale n. 33/1087 del 29.09.2023 di aggiornamento del programma biennale 2023/2024 per gli acquisti di beni e servizi di importo unitario stimato pari o superiore a € 40.000,00 ai sensi dell'art. 21, commi 1 e 6, del D.lgs. n. 50/2016;

VISTO l'art. 1 "Riduzione della spesa per l'acquisto di beni e servizi e trasparenza delle procedure" del D.L. 6 luglio 2012, n. 95, convertito, con modificazioni, dalla Legge 7 agosto 2012, n. 135, recante "Disposizioni urgenti per la revisione della spesa pubblica con invarianza dei servizi ai cittadini nonché misure di rafforzamento patrimoniale delle imprese del settore bancario";

VISTA la nota prot. n. 31/0005937 del 08.09.2015 del Segretariato Generale, con la quale è stata trasmessa la circolare congiunta del Dipartimento dell'Amministrazione Generale, del Personale e dei Servizi e del Dipartimento della Ragioneria Generale dello Stato del 25 agosto 2015, che ribadisce l'obbligo di approvvigionamento per le amministrazioni statali per il tramite di Consip S.p.A.;

VISTA la Legge di Stabilità 2016 (Legge 28 dicembre 2015, n. 208), pubblicata sulla G.U. n. 302 del 30.12.2015 - Suppl. Ordinario n. 70, che contiene una manovra di razionalizzazione dei processi di approvvigionamento di beni e servizi per le amministrazioni pubbliche;

VISTO l'art. 62 "Aggregazioni e centralizzazione delle committenze" del D.lgs. n. 36/2023;

VISTA la Legge di Stabilità 2017 (Legge 11 dicembre 2016, n. 232), pubblicata sulla GU n. 297 del 21.12.2016 - Suppl. Ordinario n. 57, che contiene ulteriori misure di razionalizzazione della spesa pubblica, con particolare riferimento all'acquisizione di beni e servizi in forma centralizzata;

VISTA la Legge di Bilancio 2018 (Legge 27 dicembre 2017, n. 205), pubblicata sulla G.U. n. 302 del 29.12.2017 - Suppl. Ordinario n. 62, che contiene ulteriori indicazioni in relazione alla centralizzazione degli acquisti;

VISTA la Legge di Bilancio 2019 (Legge 30 dicembre 2018, n. 145), pubblicata sulla G.U. n. 302 del 31 dicembre 2018 - Suppl. Ordinario n. 62;

VISTA la Legge di Bilancio 2020 (Legge 27 dicembre 2019, n. 160), pubblicata sulla G.U. n. 304 del 30 dicembre 2019 - Suppl. Ordinario n. 45;

VISTA la Legge di Bilancio 2021 (Legge 30 dicembre 2020, n. 178), pubblicata sulla G.U. n. 322 del 30 dicembre 2020 - Suppl. Ordinario n. 46;

VISTA la Legge di Bilancio 2022 (Legge 30 dicembre 2021, n. 234), pubblicata sulla G.U. n. 310 del 31 dicembre 2021 - Suppl. Ordinario n. 49;

VISTA la Legge di Bilancio 2023 (Legge 29 dicembre 2022, n. 197), pubblicata sulla G.U. n. 303 del 29 dicembre 2022 - Suppl. Ordinario n. 43;

VISTO il Decreto del Presidente del Consiglio dei ministri del 29 dicembre 2021, registrato dalla Corte dei Conti in data 20.01.2022 al n. 152, con il quale è stato conferito alla scrivente l'incarico di funzione dirigenziale di livello generale di Direttore della Direzione Generale dell'Innovazione tecnologica, delle risorse strumentali e della comunicazione;

VISTO il Decreto Direttoriale n. 499 del 3 giugno 2022, registrato alla Corte dei Conti in data 29 luglio 2022 al n. 2095, con il quale è stato conferito alla dott.ssa Stefania Rupe l'incarico di titolarità della Divisione IV "Contratti e pagamenti relativi a beni e servizi informatici e non informatici" della Direzione Generale dell'Innovazione tecnologica, delle risorse strumentali e della comunicazione, per il periodo dal 15 giugno 2022 al 14 giugno 2025;

VISTO il Decreto Direttoriale n. 884 del 13 settembre 2022, registrato, ai sensi del D.lgs. n. 123 del 30 giugno 2011, al n. 427 del 23 settembre 2022, con il quale la dott.ssa Stefania Rupe - Dirigente della Divisione IV

della Direzione Generale dell'innovazione tecnologica, delle risorse strumentali e della comunicazione, è delegata alla firma degli atti della suindicata Divisione;

VISTO il Decreto Direttoriale n. 302 del 23 marzo 2023, registrato, ai sensi del D.lgs. n. 123 del 30 giugno 2011, al n. 132 del 24 marzo 2023, con il quale la dott.ssa Stefania Rupe è delegata alla firma degli atti amministrativo contabili, inerenti ai capitoli di spesa di competenza della Direzione Generale dell'Innovazione tecnologica, delle risorse strumentali e della comunicazione, così come individuati nell'Allegato C del Decreto del Ministro del lavoro e delle politiche sociali n. 12 dell'8 febbraio 2023 di assegnazione risorse, nonché a quelli in gestione unificata, così come individuati nell'Allegato B al Decreto Ministeriale n. 29 dell'8 marzo 2023, concernente la gestione unificata delle spese comuni ai Centri di Responsabilità Amministrativa per l'esercizio finanziario 2023;

PRESO ATTO che, con nota protocollo n. 31/7597 del 04.10.2016 avente ad oggetto "Indicazioni in materia di affidamenti a soggetti esterni", il Segretariato Generale, in un'ottica di maggiore responsabilizzazione delle strutture interne volte all'effettiva attuazione del principio di buona amministrazione, come ribadito anche dalla Determinazione dell'ANAC n. 12 del 28 ottobre 2015, ha richiesto l'esplicitazione formale dei motivi sottesi al ricorso alla commessa pubblica attraverso una rappresentazione qualitativa e quantitativa del fabbisogno interno in termini di beni e servizi da affidare;

CONSIDERATO che, nel corso degli ultimi anni, gli attacchi *hacker* sono aumentati in modo considerevole ponendo ancora di più l'attenzione sulla tematica della sicurezza informatica, in relazione alla quale questo Ministero ha adottato una serie di misure che vanno dalla formazione del personale sui rischi della rete alla protezione dei sistemi attraverso l'acquisto di soluzioni specifiche;

CONSIDERATO che le nuove modalità di attacco dimostrano che i *cyber* criminali sono sempre più sofisticati e in grado di fare rete con la criminalità organizzata;

CONSIDERATO che, nell'attuale panorama digitale, una crescente minaccia è rappresentata dal "furto di identità", attraverso il quale i *cyber* criminali accedono illegalmente e senza autorizzazione alle informazioni personali di un altro individuo;

CONSIDERATO che le identità con privilegi sono il principale vettore per il *ransomware* (programma informatico "malevolo" che può infettare un dispositivo digitale e bloccare l'accesso a tutti o ad alcuni dei suoi contenuti) e altri attacchi informatici mirati;

CONSIDERATO che, sempre negli ultimi anni, i cyber criminali hanno focalizzato la loro attenzione non più sui sistemi ma sugli attacchi basati sull'identità, una tendenza che ha portato a un contestuale aumento degli attacchi informatici spesso non rilevati, in quanto non lasciano indicatori di compromissione o prove di *malware*;

CONSIDERATO che, nonostante l'implementazione di soluzioni di gestione degli account con privilegi e di autenticazione a due o più fattori, un endpoint su sei rileva rischi legati all'identità con privilegi;

CONSIDERATO che, da anni, il Ministero del lavoro e delle politiche sociali ha innalzato il livello di protezione e di reazione sui temi di cyber-security al fine di rispondere in modo efficace in caso di minacce digitali;

CONSIDERATO che, in attuazione di quanto sopra rappresentato, il Ministero del lavoro e delle politiche sociali, con Decreto Direttoriale prot. n. 33/1510 del 21.12.2022 e conseguente Contratto Esecutivo prot. n. 33/8987 del 23.12.2022, ha perfezionato l'adesione all'Accordo Quadro Consip "Servizi di sicurezza da remoto, compliance e controllo per le pubbliche amministrazioni - ID 2296" - Lotto 2 - Servizi di compliance e controllo, con l'obiettivo di garantire la mappatura dell'esposizione a minacce *cyber* e la relativa tenuta dei

servizi informatici e telematici allineando il proprio modello organizzativo di sicurezza ICT alle linee guida, alle direttive e alle normative di livello nazionale ed europeo;

CONSIDERATO, inoltre, che il Ministero del lavoro e delle politiche sociali, a seguito della concessione del lavoro agile ai propri dipendenti, con Decreto Direttoriale prot. n. 33/247 del 10.03.2023 e conseguente documento di stipula prot. n. 33/2472 del 29.03.2023 ha proceduto ad acquisire le licenze collegate alla piattaforma *Cyber guru*, una soluzione di E-learning capace di trasformare i comportamenti del personale dipendente grazie ad un percorso di apprendimento educativo sulle norme di sicurezza informatica, consentendo di proteggere i propri dati e le cartelle di rete dai rischi derivanti dal *cyber crime*;

CONSIDERATO che, alla luce del contesto rappresentato e della necessità di mantenere un elevato standard di protezione dalle minacce dei *cyber* criminali, il Ministero del lavoro e delle politiche sociali ha la necessità di acquisire una soluzione software che consenta di utilizzare una piattaforma informatica in grado di analizzare e contestualizzare i rischi associati alle identità digitali presenti nei dispositivi IT, utilizzati all'interno dell'infrastruttura IT di questa Amministrazione, siano essi server fisici o virtuali, laptop o desktop;

CONSIDERATO che la soluzione ricercata da questa Amministrazione consentirebbe, inoltre, di ottenere indicazioni utili per rimediare e mettere in sicurezza le identità classificate a rischio, ricercando tutte quelle identità informatiche che potrebbero essere sfruttate da eventuali attaccanti o da utenti malintenzionati;

INDIVIDUATA dai referenti tecnici di questa Amministrazione, quale soluzione tecnica maggiormente idonea a soddisfare le esigenze sopra citate, la componente *Spotlight* a marchio *Proofpoint* denominata "*Identity Threat Detection and Response (ITDR)*";

CONSIDERATO che la soluzione individuata è caratterizzata da una serie di componenti, descritte nella sotto estesa tabella:

Codice	Descrizione	Quantità
PP-M-SPLT-V-A-302	ProofPoint Spotlight	2500
PP-PST-IS-IMP	InfoSec PS Implementation Services	1
PP-SUP-PS-36	PFPT Platinum Level Support	1

CONSIDERATO che la soluzione in parola, per tutti i codici e i servizi oggetto dell'affidamento, è della durata di 36 (trentasei) mesi a far data dal 01.11.2023;

CONSIDERATO che, nel corso dei 36 (trentasei) mesi, dovranno essere garantiti anche i seguenti servizi professionali: *i*) supporto tecnico accessibile ed attivabile nella modalità 24x7 (H24 per 365 gg. all'anno); *ii*) disponibilità di tutti gli aggiornamenti dei prodotti e delle release successive;

CONSIDERATO che la soluzione tecnologica individuata è articolata in due componenti che verranno installate su server (anche virtuali) messi a disposizione da questa Amministrazione: *i*) Identity Threat and Response Dashboard Server; *ii*) Spotlight Server;

CONSIDERATO che la piattaforma di controllo e gestione dovrà essere installata all'interno dei Datacenter del Ministero del lavoro e delle politiche sociali e avrà il compito di interagire con gli altri elementi presenti all'interno dello stesso (Active Directory, PAM, SIEM etc..), rendendo fruibile per il gruppo di conduzione IT del Centro Servizi Informatici tutte le informazioni di dettaglio sulle identità a rischio analizzate dalla piattaforma Illusive *Spotlight;*

CONSIDERATO che la soluzione ITDR di Proofpoint dovrà evidenziare tutti i rischi associati alle identità andando a identificare potenziali rischi quali a titolo esemplificativo: *i*) Account local admin non gestiti; *ii*) Service-Account non gestiti o che presentano delle errate configurazioni sui privilegi/password; *iii*) Credenziali di amministratore di dominio memorizzate nella cache contenute degli endpoint; *iv*) Utenti privilegiati non gestiti; *v*) Sessioni RDP disconnesse in modo errato con accessi sfruttabili da attaccanti; *vi*) Shadow Admin a rischio o con privilegi elevati;

RILEVATO che la piattaforma *Proofpoint* ITDR consentirà non solo di identificare tutte le vulnerabilità associabili alle identità sfruttabili da un eventuale attaccante, ma dovrà fornire anche il dettaglio di quali possibili attacchi informatici potrebbero essere eseguiti, mappandoli anche allo standard associato descritto secondo il "*Mitre att&ck*" e, al tempo stesso, dovrà fornire la possibile o le possibili azioni (*remediation*) per mettere in sicurezza la criticità evidenziata;

CONSIDERATO che gli obiettivi principali che si intendono conseguire mediante la soluzione individuata sono: *i*) accrescere il livello di sicurezza nelle piattaforme che gestiscono le identità informatiche con una valutazione e mitigazione del rischio cyber; *ii*) adottare metodologie, processi e strumenti capaci di ridurre il rischio di esposizione di identità deboli o sfruttabili in caso di attacchi informatici; *iii*) verificare ricorsivamente e in maniera esaustiva l'eventuale presenza di eventuali identità a rischio che possono insorgere dalle attività quotidiane nella gestione delle piattaforme e dei sistemi; *iv*) intervenire proattivamente e tempestivamente in caso di identificazione di identità a rischio;

CONSIDERATO che la casa madre *Proofpoint* rende disponibili le licenze ricercate dall'Amministrazione attraverso una rete di rivenditori ufficiali;

CONSIDERATO che l'art. 79 del D.lgs. n. 36/2023, concernente le "*Specifiche tecniche*", il quale rimanda all'Allegato II.5, PARTE II, A – SPECIFICHE TECNICHE, comma 6, prescrive di indicare la motivazione eccezionale dell'indicazione del marchio del prodotto qualora non possa essere applicato il precedente comma 5;

DATO ATTO che il riferimento al marchio "*Proofpoint*" è motivato dal fatto che questa Direzione Generale ha individuato la soluzione *Spotlight* a marchio Proofpoint come rispondente al proprio fabbisogno, in quanto funzionale a consentire la ricerca di tutte quelle identità informatiche che potrebbero essere sfruttate da eventuali attaccanti o da utenti malintenzionati, rispondendo in modo efficace a fronte di eventuali minacce digitali;

CONSIDERATO che, per il raggiungimento delle finalità sopra elencate, è necessario acquisire la componente *Spotlight* a marchio *Proofpoint* denominata "*Identity Threat Detection and Response (ITDR)*" ed i servizi professionali connessi da un operatore specializzato;

VISTO l'art. 50 del D.lgs. n. 36/2023 che dispone, al comma 1, lettera b), che le stazioni appaltanti procedano mediante affidamento diretto per i servizi e le forniture di importo inferiore a 140.000 euro, anche senza consultazione di più operatori economici, assicurando che siano scelti soggetti in possesso di documentate esperienze pregresse idonee all'esecuzione delle prestazioni contrattuali, anche individuati tra gli iscritti in elenchi o albi istituiti dalla stazione appaltante;

VISTO l'art. 17, comma 2 del D.lgs. n. 36/2023 il quale dispone che, in caso di affidamento diretto, la stazione appaltante individui nella decisione di contrarre l'oggetto, l'importo e il contraente, unitamente alle ragioni della sua scelta, ai requisiti di carattere generale e, se necessari, a quelli inerenti alla capacità economico-finanziaria e tecnico-professionale;

CONSIDERATO che la soluzione rappresenta un nuovo acquisto per l'amministrazione e non un rinnovo, questa Direzione ha inteso acquisire dalla casa madre l'elenco ufficiale dei partner ed ha inteso procedere

individuando società in possesso di un curriculum aziendale con comprovate esperienze rispetto all'oggetto dell'affidamento;

INDIVIDUATE, nello specifico, la LumIT S.p.A., con sede in Roma alla Via Bartolomeo D'Alviano, 71/A – P.IVA 06745090966, e la Telsy S.p.A., con sede in Torino in Corso Svizzera, 185 – P.IVA. 00737690016;

VISTE:
- la richiesta di offerta inviata, con nota prot. 33/6659 del 18.09.2023, alla LumIT S.p.A., con sede in Roma alla Via Bartolomeo D'Alviano, 71/A – P.IVA 06745090966 avente ad oggetto la trasmissione della propria migliore offerta economica per l'acquisizione della "*fornitura della componente Spotlight della Proofpoint Identity Threat Detection and Response (ITDR)*";
- la richiesta di offerta inviata, con nota prot. 33/6658 del 18.09.2023, alla Telsy S.p.A., con sede in Torino in Corso Svizzera, 185 – P.IVA. 00737690016 avente ad oggetto la trasmissione della propria migliore offerta economica per l'acquisizione della "*fornitura della componente Spotlight della Proofpoint Identity Threat Detection and Response (ITDR)*";

CONSIDERATO che entro il termine ultimo per la presentazione di un preventivo di spesa, fissato alla data del 25.09.2023, non è pervenuta all'indirizzo di posta elettronica certificata dell'Amministrazione nessuna offerta economica da parte delle sopra citate società;

CONSIDERATO che dall'elenco dei reseller ufficiali, indicato dalla casa madre *Proofpoint*, questa Amministrazione ha provveduto ad individuare ulteriori n. 3 (tre) società in possesso di un curriculum aziendale con comprovate esperienze rispetto all'oggetto dell'affidamento;

VISTE:
- la richiesta di offerta inviata, con nota prot. 33/6905 del 26.09.2023, alla 7Layers S.r.l., con sede in Brembate (BG) in Piazza Adriano Olivetti, 1 – P.IVA 06225550489 avente ad oggetto la trasmissione della propria migliore offerta economica per l'acquisizione della "*fornitura della componente Spotlight della Proofpoint Identity Threat Detection and Response (ITDR)*";
- la richiesta di offerta inviata, con nota prot. 33/6907 del 26.09.2023, alla HWG S.r.l., con sede in Verona alla Via Enrico Fermi, 15/E – P.IVA. 03820790230 avente ad oggetto la trasmissione della propria migliore offerta economica per l'acquisizione della "*fornitura della componente Spotlight della Proofpoint Identity Threat Detection and Response (ITDR)*";
- la richiesta di offerta inviata, con nota prot. 33/6908 del 26.09.2023, alla Sorint.Sec S.r.l., con sede in Brembate (BG) alla Via Vittorio Veneto, 25 – P.IVA. 04010360164 avente ad oggetto la trasmissione della propria migliore offerta economica per l'acquisizione della "*fornitura della componente Spotlight della Proofpoint Identity Threat Detection and Response (ITDR)*";

CONSIDERATO che in data 28.09.2023, entro il termine fissato al 02.10.2023, è pervenuta all'indirizzo di posta elettronica certificata dell'Amministrazione l'offerta economica presentata dalla HWG S.r.l., con sede in Verona alla Via Enrico Fermi, 15/E – P.IVA. 03820790230, pari a € 134.000,00 (centotrentaquattromila/00) IVA esclusa, acquisita al protocollo di questa Direzione Generale in pari data con il n. 33/6986;

PRESO ATTO degli esiti dell'istruttoria svolta per l'individuazione di un operatore economico specializzato a cui affidare il servizio di cui trattasi;

DATO ATTO che il servizio di cui trattasi non rientra nell'ambito di applicazione dei criteri minimi ambientali in base al Piano per la sostenibilità ambientale dei consumi del settore della Pubblica Amministrazione;

DATO ATTO che non sussistono convenzioni stipulate da Consip in relazione al servizio di cui trattasi;

DATO ATTO che si è proceduto a visionare sul Mercato elettronico della pubblica amministrazione (MePA) l'iniziativa "SERVIZI" e, nello specifico, la categoria "Sicurezza Informatica-Mepa servizi", pertinente per l'acquisizione in parola;

CONSIDERATO che la HWG S.r.l., con sede in Verona alla Via Enrico Fermi, 15/E – P.IVA. 03820790230, è un provider di cybersecurity che offre una suite completa di strategie di sicurezza, servizi gestiti e consulenza con particolare attenzione alle soluzioni di cybersecurity integrate e personalizzate per la protezione di ambienti IT, OT e IoT dalle minacce informatiche;

CONSIDERATO che la HWG S.r.l. opera in oltre 20 Paesi nel mondo, proteggendo le infrastrutture digitali di organizzazioni in vari settori;

CONSIDERATO che la HWG S.r.l., come da informazioni rinvenibili sul sito https://www.hwgsababa.com/, è in possesso di molteplici certificazioni di qualità: Quality Management System (ISO 9001), Service Management System (ISO 20000), Business Continuity Management System (ISO 22301), Information Security Management Systems (ISO 27001), STATUS LISTED TI - circuito dell'European Union Agency for Cybersecurity (ENISA), Cybersecurity made in Europe - etichetta di qualità per le aziende del settore cybersecurity erogata in Italia dal Comitato Nazionale per la Ricerca in Cybersecurity;

DATO ATTO che è stata verificata la regolarità contributiva della HWG S.r.l. mediante acquisizione del DURC, prot. INPS_36730734, rilasciato in data 04.07.2023, in corso di validità, e custodito agli atti degli Uffici di questa Direzione;

ACCERTATA, per quanto sopra, l'affidabilità e l'idoneità della HWG S.r.l. rispetto all'erogazione del servizio di cui trattasi essendo questa in possesso di pregresse e documentate esperienze idonee all'esecuzione delle prestazioni contrattuali, come richiesto dal citato art. 50, comma 1, lett. b) del D.lgs. n. 36/2023;

CONSIDERATO che il costo complessivo stimato per l'acquisto dei servizi richiesti è stato stimato in € 134.000,00 (centotrentaquattromila/00) IVA esclusa;

CONSIDERATO che, al fine di verificare la corretta congruità della spesa, questa Direzione ha valutato la necessità di far precedere la Trattativa Diretta da richieste di offerta ai reseller autorizzati;

CONSIDERATO che per l'esecuzione del servizio la HWG S.r.l. ha offerto un importo complessivo pari a € 134.000,00 (centotrentaquattromila/00) IVA esclusa, come indicato nell'offerta economica protocollo n. 33/6986 del 28.09.2023;

DETERMINATO, pertanto, il costo complessivo del servizio in € 134.000,00 (centotrentaquattromila/00) IVA esclusa, come da offerta economica trasmessa dalla HWG S.r.l. (protocollo n. 33/6986 del 28.09.2023);

DATO ATTO che la congruità del prezzo è stata verificata in relazione ad affidamenti similari effettuati negli ultimi anni, alla tipologia, alla durata del servizio richiesto nonché al preventivo di spesa trasmesso dalla HWG S.r.l.;

CONSIDERATO che gli esiti dell'istruttoria sono conformi al principio del risultato enunciato dall'art.1 del D.lgs. n. 36/2023;

ACCERTATO, per tutto quanto sopra, che ricorrono i presupposti di legge per l'acquisizione del suddetto servizio mediante affidamento diretto, nel rispetto dei principi di cui al Libro I, Parti I e II, richiamati agli artt. 48, comma 1 e 49, comma 4 del D.lgs. n. 36/2023, nonché del rispetto di quanto indicato nell'allegato II.1 del D.lgs. n. 36/2023;

RITENUTO che lo strumento denominato "Trattativa Diretta", tra quelli messi a disposizione da Consip S.p.A. sulla piattaforma www.acquistinretepa.it del MePA, è il più idoneo all'esperimento di una procedura negoziata con un unico operatore, in quanto consente all'Amministrazione di contrattare direttamente con l'operatore economico individuato, sulla base delle valutazioni effettuate in relazione alle proprie specifiche esigenze;

RITENUTO, pertanto, opportuno procedere all'affidamento del servizio di cui trattasi mediante ricorso allo strumento denominato "Trattativa Diretta" con la HWG S.r.l.;

ATTESO che al contratto saranno applicabili le Condizioni generali relative al bando "SERVIZI";

VISTI gli atti predisposti a questo effetto dagli Uffici di questa Direzione e, in particolare, il documento "Specifiche Tecniche", nel quale sono indicate le condizioni del servizio e le attività richieste alla società affidataria;

CONSIDERATO che per la spesa in oggetto non risulta necessaria l'acquisizione del CUP trattandosi di Fondi di Bilancio del Ministero del Lavoro e delle Politiche Sociali;

CONSIDERATO che è stato acquisito il CIG A01D2CE8FC, tramite il sistema SIMOG di ANAC, sia ai fini della tracciabilità dei flussi di cui alla Legge 136/2010 che del monitoraggio dei contratti pubblici;

VISTO l'art. 18, comma 1 del D.lgs. n. 36/2023 che prevede, in caso di procedure negoziate, la stipula del contratto mediante corrispondenza secondo l'uso commerciale, consistente in un apposito scambio di lettere, anche tramite posta elettronica certificata o sistemi elettronici di recapito certificato qualificato ai sensi del Regolamento UE n. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014;

Tanto premesso,

D E C R E T A

Articolo 1

La Direzione Generale dell'Innovazione tecnologica, delle risorse strumentali e della comunicazione:

i. procede all'acquisizione delle "*fornitura della componente Spotlight della Proofpoint Identity Threat Detection and Response (ITDR)"* mediante Trattativa diretta sul Mercato elettronico della Pubblica Amministrazione (MePA) gestito da Consip S.p.A., iniziativa "SERVIZI", categoria "Sicurezza Informatica-Mepa servizi", ai sensi dell'art. 50, comma 1, lett. b) del D.lgs. n. 36/2023, per un importo complessivo di € 134.000,00 (centotrentaquattromila/00) IVA esclusa, CIG A01D2CE8FC;
ii. a tal fine ha individuato la HWG S.r.l., con sede in Verona alla Via Enrico Fermi, 15/E – P.IVA. 03820790230;

Articolo 2

Il Responsabile Unico del Progetto (RUP) ai sensi dell'art. 15 del D.lgs. n. 36/2023 è la dott.ssa Maria Condemi, Direttore Generale della Direzione Generale dell'Innovazione tecnologica, delle risorse strumentali e della comunicazione.

Articolo 3

Il Responsabile del procedimento per la fase di affidamento ai sensi dell'art. 15, comma 4 del D.lgs. n. 36/2023 è la Dott.ssa Stefania Rupe, Dirigente della Divisione IV della Direzione Generale dell'innovazione tecnologica, delle risorse strumentali e della comunicazione.

Articolo 4

La spesa necessaria per finanziare l'operazione descritta in premessa verrà posta a carico del capitolo di Bilancio 1746 del Ministero del lavoro e delle politiche sociali per l'esercizio finanziario 2023;

Il Direttore Generale
Dott.ssa Maria Condemi*

**Documento firmato digitalmente secondo le indicazioni sulla dematerializzazione ai sensi e per gli effetti degli artt. 20 e 21 del D.lgs. n. 82/2005 "Codice dell'Amministrazione Digitale" e s.m.i.*