Rif: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

Traduzione italiana mediante Google Translator

Ordine esecutivo sul miglioramento della sicurezza informatica della nazione

12 maggio 2021

In base all'autorità conferitami in qualità di Presidente dalla Costituzione e dalle leggi degli Stati Uniti d'America, si ordina quanto segue:

Sezione 1. Politica. Gli Stati Uniti devono affrontare campagne informatiche dannose persistenti e sempre più sofisticate che minacciano il settore pubblico, il settore privato e, in ultima analisi, la sicurezza e la privacy del popolo americano. Il governo federale deve intensificare i propri sforzi per identificare, scoraggiare, proteggere, rilevare e rispondere a queste azioni e attori. Il governo federale deve anche esaminare attentamente ciò che è accaduto durante qualsiasi incidente informatico importante e applicare le lezioni apprese. Ma la sicurezza informatica richiede più dell'azione del governo. La protezione della nostra nazione da cyber-attori dannosi richiede al governo federale di collaborare con il settore privato. Il settore privato deve adattarsi al contesto delle minacce in continua evoluzione, garantire che i suoi prodotti siano costruiti e funzionino in modo sicuro e collaborare con il governo federale per promuovere un cyberspazio più sicuro.Alla fine, la fiducia che riponiamo nella nostra infrastruttura digitale dovrebbe essere proporzionale a quanto sia affidabile e trasparente tale infrastruttura e alle conseguenze che incorreremo se tale fiducia è mal riposta.

I miglioramenti incrementali non ci daranno la sicurezza di cui abbiamo bisogno; invece, il governo federale ha bisogno di fare cambiamenti coraggiosi e investimenti significativi per difendere le istituzioni vitali che sono alla base dello stile di vita americano. Il governo federale deve far valere l'intero ambito delle proprie autorità e risorse per proteggere e proteggere i propri sistemi informatici, siano essi basati su cloud, locali o ibridi. L'ambito di protezione e sicurezza deve includere i sistemi che elaborano i dati (tecnologia dell'informazione (IT)) e quelli che gestiscono i macchinari vitali che garantiscono la nostra sicurezza (tecnologia operativa (OT)).

È politica della mia amministrazione che la prevenzione, il rilevamento, la valutazione e la riparazione degli incidenti informatici sia una priorità assoluta ed essenziale per la sicurezza nazionale ed economica. Il governo federale deve dare l'esempio. Tutti i sistemi informativi federali devono soddisfare o superare gli standard e i requisiti per la sicurezza informatica stabiliti e rilasciati in base a questo ordine.

Sec. 2. Rimozione degli ostacoli alla condivisione delle informazioni sulle minacce.

(a) Il governo federale stipula un contratto con i fornitori di servizi IT e OT per condurre una serie di funzioni quotidiane sui sistemi informativi federali. Questi fornitori di servizi, inclusi i fornitori di servizi cloud, hanno un accesso unico e una visione delle informazioni sulle minacce informatiche e sugli incidenti sui sistemi informativi federali. Allo stesso tempo, le attuali clausole contrattuali o restrizioni possono limitare la condivisione di tali informazioni su minacce o incidenti con i dipartimenti esecutivi e le agenzie (agenzie) responsabili delle indagini o della riparazione degli incidenti informatici, come la Cybersecurity and Infrastructure Security Agency (CISA), il

Federal Bureau of Investigation (FBI) e altri elementi della Intelligence Community (IC). Rimuovere queste barriere contrattuali e aumentare la condivisione di informazioni su tali minacce, incidenti,ei rischi sono passaggi necessari per accelerare la deterrenza, la prevenzione e gli sforzi di risposta agli incidenti e per consentire una difesa più efficace dei sistemi delle agenzie e delle informazioni raccolte, elaborate e mantenute da o per il governo federale.

(b) Entro 60 giorni dalla data di questo ordine, il Direttore dell'Office of Management and Budget (OMB), in consultazione con il Segretario della Difesa, il Procuratore generale, il Segretario della Sicurezza interna e il Direttore dell'intelligence nazionale , esaminerà i requisiti del contratto FAR (Federal Acquisition Regulation) e del Supplemento al regolamento federale sull'acquisizione della difesa e la lingua per i contratti con i fornitori di servizi IT e OT e raccomanderà aggiornamenti a tali requisiti e lingua al Consiglio FAR e ad altre agenzie appropriate. Le raccomandazioni devono includere le descrizioni degli appaltatori che devono essere coperti dalla lingua contrattuale proposta.

(c) La lingua contrattuale raccomandata ei requisiti descritti nella sottosezione (b) di questa sezione devono essere progettati per garantire che:

i) i fornitori di servizi raccolgono e conservano dati, informazioni e rapporti rilevanti per la prevenzione, il rilevamento, la risposta e l'indagine di eventi di sicurezza informatica su tutti i sistemi di informazione sui quali hanno il controllo, compresi i sistemi gestiti per conto delle agenzie, in linea con i requisiti delle agenzie;

(ii) i fornitori di servizi condividono tali dati, informazioni e rapporti, in quanto si riferiscono a incidenti informatici o potenziali incidenti rilevanti per qualsiasi agenzia con cui hanno stipulato un contratto, direttamente con tale agenzia e qualsiasi altra agenzia che il Direttore di OMB, in consultazione con il Segretario della Difesa, il Procuratore generale, il Segretario per la sicurezza interna e il Direttore dell'intelligence nazionale, ritengono appropriato, coerente con le leggi, i regolamenti e le politiche sulla privacy applicabili;

(iii) i fornitori di servizi collaborano con le agenzie di sicurezza informatica o investigative federali nelle loro indagini e risposte a incidenti o potenziali incidenti sui sistemi di informazione federali, anche implementando capacità tecniche, come il monitoraggio delle reti per le minacce in collaborazione con le agenzie che supportano, se necessario; e

(iv) i fornitori di servizi condividono le informazioni sulle minacce informatiche e sugli incidenti con le agenzie, facendo ciò, ove possibile, in formati riconosciuti dal settore per la risposta agli incidenti e la riparazione.

(d) Entro 90 giorni dal ricevimento delle raccomandazioni descritte nella sottosezione (b) di questa sezione, il Consiglio FAR rivedrà la lingua e le condizioni del contratto proposto e, se del caso, pubblicherà per il commento pubblico gli aggiornamenti proposti al FAR.

(e) Entro 120 giorni dalla data di questo ordine, il Segretario della Sicurezza Nazionale e il Direttore dell'OMB prenderanno le misure appropriate per garantire nella massima misura possibile che i fornitori di servizi condividano i dati con le agenzie, la CISA e l'FBI, a seconda dei casi. necessario al governo federale per rispondere a minacce, incidenti e rischi informatici.

(f) È politica del governo federale che:

(i) i fornitori di servizi di tecnologia dell'informazione e della comunicazione (TIC) che stipulano contratti con le agenzie devono riferire prontamente a tali agenzie quando scoprono un incidente informatico che coinvolge un prodotto o servizio software fornito a tali agenzie o che coinvolgono un sistema di supporto per un prodotto o servizio software fornito a tali agenzie;

(ii) i fornitori di servizi ICT devono anche riferire direttamente alla CISA ogni volta che fanno rapporto ai sensi della sottosezione (f) (i) di questa sezione alle agenzie del ramo esecutivo civile federale (FCEB) e la CISA deve raccogliere e gestire a livello centrale tali informazioni; e

(iii) i rapporti relativi ai Sistemi di Sicurezza Nazionale, come definiti nella sezione 10 (h) del presente ordine, devono essere ricevuti e gestiti dall'agenzia appropriata come da determinare ai sensi della sottosezione (g) (i) (E) di questa sezione .

(g) Per implementare la politica stabilita nella sottosezione (f) di questa sezione:

(i) Entro 45 giorni dalla data di questo ordine, il Segretario della Sicurezza Nazionale, in consultazione con il Segretario della Difesa che agisce tramite il Direttore dell'Agenzia per la Sicurezza Nazionale (NSA), il Procuratore Generale e il Direttore dell'OMB, dovrà raccomandare al Consiglio FAR un linguaggio contrattuale che identifichi:

(A) la natura degli incidenti informatici che richiedono la segnalazione;

(B) i tipi di informazioni sugli incidenti informatici che richiedono la segnalazione per facilitare un'efficace risposta e riparazione agli incidenti informatici;

(C) protezioni adeguate ed efficaci per la privacy e le libertà civili;

(D) i periodi di tempo entro i quali gli appaltatori devono segnalare gli incidenti informatici sulla base di una scala graduata di gravità, con la segnalazione degli incidenti informatici più gravi che non devono superare i 3 giorni dopo il rilevamento iniziale;

(E) requisiti di segnalazione dei sistemi di sicurezza nazionale; e

(F) il tipo di appaltatori e fornitori di servizi associati che devono essere coperti dalla lingua contrattuale proposta.

(ii) Entro 90 giorni dal ricevimento delle raccomandazioni descritte nella sottosezione (g) (i) di questa sezione, il Consiglio FAR esaminerà le raccomandazioni e pubblicherà per il commento pubblico gli aggiornamenti proposti al FAR.

(iii) Entro 90 giorni dalla data di questo ordine, il Segretario della Difesa che agisce tramite il Direttore della NSA, il Procuratore generale, il Segretario della Sicurezza interna e il Direttore dell'intelligence nazionale svilupperà congiuntamente procedure per garantire tale incidente informatico le relazioni sono tempestivamente e adeguatamente condivise tra le agenzie.

(h) Gli attuali requisiti di sicurezza informatica per i contratti di sistema non classificati sono ampiamente implementati attraverso politiche e regolamenti specifici dell'agenzia, compresi i requisiti di sicurezza informatica dei servizi cloud. La standardizzazione dei requisiti contrattuali di sicurezza informatica comuni tra le agenzie semplificherà e migliorerà la conformità per i fornitori e il governo federale.

(i) Entro 60 giorni dalla data di questo ordine, il Segretario della Sicurezza Nazionale che agisce tramite il Direttore della CISA, in consultazione con il Segretario della Difesa che agisce tramite il Direttore della NSA, il Direttore dell'OMB e l'Amministratore del Generale I servizi devono riesaminare i requisiti di sicurezza informatica specifici dell'agenzia che attualmente esistono per legge, politica o contratto e raccomandano al Consiglio delle FAR un linguaggio contrattuale standardizzato per i requisiti di sicurezza informatica appropriati. Tali raccomandazioni devono includere la considerazione della portata dei contraenti e dei fornitori di servizi associati che devono essere coperti dalla lingua del contratto proposta.

(j) Entro 60 giorni dal ricevimento della lingua contrattuale raccomandata sviluppata ai sensi della sottosezione (i) di questa sezione, il Consiglio FAR rivedrà la lingua contrattuale raccomandata e pubblicherà per il commento pubblico gli aggiornamenti proposti al FAR.

(k) A seguito di eventuali aggiornamenti al FAR effettuati dal Consiglio FAR dopo il periodo di commento pubblico descritto nella sottosezione (j) di questa sezione, le agenzie aggiornano i requisiti di sicurezza informatica specifici dell'agenzia per rimuovere eventuali requisiti duplicati di tali aggiornamenti FAR.

(l) Il Direttore dell'OMB deve incorporare nel processo di bilancio annuale un'analisi dei costi di tutte le raccomandazioni sviluppate in questa sezione.

Sec. 3. Modernizzazione della sicurezza informatica del governo federale.

(a) Per stare al passo con l'attuale ambiente dinamico e sempre più sofisticato delle minacce informatiche, il governo federale deve adottare misure decisive per modernizzare il suo approccio alla sicurezza informatica, anche aumentando la visibilità del governo federale sulle minacce, proteggendo la privacy e le libertà civili. Il governo federale deve adottare le migliori pratiche di sicurezza; avanzare verso Zero Trust Architecture; accelerare il passaggio alla protezione dei servizi cloud, inclusi Software as a Service (SaaS), Infrastructure as a Service (IaaS) e Platform as a

Service (PaaS); centralizzare e semplificare l'accesso ai dati sulla sicurezza informatica per guidare l'analisi per identificare e gestire i rischi per la sicurezza informatica; e investire in tecnologia e personale per raggiungere questi obiettivi di modernizzazione.

(b) Entro 60 giorni dalla data di questo ordine, il capo di ciascuna agenzia deve:

(i) aggiornare i piani dell'agenzia esistenti per dare la priorità alle risorse per l'adozione e l'uso della tecnologia cloud come delineato nelle pertinenti linee guida dell'OMB;

(ii) sviluppare un piano per implementare Zero Trust Architecture, che includerà, come appropriato, le fasi di migrazione che il National Institute of Standards and Technology (NIST) all'interno del Dipartimento del Commercio ha delineato negli standard e nelle linee guida, descrivere tali passaggi che sono già state completate, identificare le attività che avranno l'impatto più immediato sulla sicurezza e includere un programma per implementarle; e

(iii) fornire un rapporto al Direttore dell'OMB e all'Assistente del Presidente e del Consigliere per la sicurezza nazionale (APNSA) che discute i piani richiesti ai sensi della sottosezione (b) (i) e (ii) di questa sezione.

(c) Man mano che le agenzie continuano a utilizzare la tecnologia cloud, lo faranno in modo coordinato e deliberato che consenta al governo federale di prevenire, rilevare, valutare e porre rimedio agli incidenti informatici. Per facilitare questo approccio, la migrazione alla tecnologia cloud adotterà l'architettura Zero Trust, come possibile. Il CISA modernizzerà i suoi attuali programmi, servizi e capacità di sicurezza informatica per essere completamente funzionali con ambienti di cloud computing con Zero Trust Architecture. Il Segretario della Sicurezza Nazionale che agisce tramite il Direttore della CISA, in consultazione con l'Amministratore dei Servizi Generali che agisce attraverso il Programma Federale di Gestione dei Rischi e delle Autorizzazioni (FedRAMP) all'interno dell'Amministrazione dei Servizi Generali,svilupperà principi di sicurezza che disciplinano i fornitori di servizi cloud (CSP) da incorporare negli sforzi di modernizzazione dell'agenzia. Per facilitare questo lavoro:

(i) Entro 90 giorni dalla data di questo ordine, il Direttore dell'OMB, in consultazione con il Segretario della Sicurezza Nazionale che agisce tramite il Direttore della CISA, e l'Amministratore dei Servizi Generali che agisce tramite FedRAMP, svilupperà una sicurezza cloud federale strategia e fornire orientamenti alle agenzie di conseguenza. Tale guida dovrà cercare di garantire che i rischi per FCEB derivanti dall'utilizzo di servizi basati su cloud siano ampiamente compresi e affrontati in modo efficace e che le Agenzie FCEB si avvicinino all'architettura Zero Trust.

(ii) Entro 90 giorni dalla data di questo ordine, il Segretario della Sicurezza Nazionale che agisce tramite il Direttore della CISA, in consultazione con il Direttore dell'OMB e l'Amministratore dei Servizi Generali che agisce tramite FedRAMP, svilupperà ed emetterà, per la FCEB , documentazione sull'architettura di riferimento tecnica per la sicurezza del cloud che illustra gli approcci consigliati alla migrazione al cloud e alla protezione dei dati per la raccolta e il reporting dei dati dell'agenzia.

(iii) Entro 60 giorni dalla data del presente ordine, il Segretario della Sicurezza Nazionale che agisce tramite il Direttore della CISA svilupperà ed emetterà, per le Agenzie FCEB, un quadro di governance dei servizi cloud. Tale quadro identifica una gamma di servizi e protezioni disponibili per le agenzie in base alla gravità dell'incidente. Tale quadro identifica anche i dati e le attività di trattamento associate a tali servizi e protezioni.

(iv) Entro 90 giorni dalla data di questo ordine, i capi delle Agenzie FCEB, in consultazione con il Segretario della Sicurezza Nazionale che agisce tramite il Direttore della CISA, valuteranno i tipi e la sensibilità dei dati non classificati della loro rispettiva agenzia e forniranno al Segretario della Sicurezza Nazionale tramite il Direttore della CISA e al Direttore dell'OMB un rapporto basato su tale valutazione. La valutazione deve dare la priorità all'identificazione dei dati non classificati considerati dall'agenzia come i più sensibili e maggiormente minacciati e soluzioni di elaborazione e archiviazione appropriate per tali dati.

(d) Entro 180 giorni dalla data di questo ordine, le agenzie adotteranno l'autenticazione a più fattori e la crittografia per i dati a riposo e in transito, nella misura massima coerente con le leggi sui

registri federali e altre leggi applicabili. A tal fine:

(i) i capi delle agenzie FCEB forniranno rapporti al segretario della sicurezza interna tramite il direttore della CISA, il direttore dell'OMB e l'APNSA sui progressi delle rispettive agenzie nell'adozione dell'autenticazione multifattoriale e della crittografia dei dati a riposo e in transito. Tali agenzie forniranno tali rapporti ogni 60 giorni dopo la data del presente ordine fino a quando l'agenzia non avrà adottato completamente l'autenticazione a più fattori e la crittografia dei dati a livello di agenzia.

(ii) Sulla base delle lacune individuate nell'implementazione dell'agenzia, la CISA deve adottare tutte le misure appropriate per massimizzare l'adozione da parte delle agenzie FCEB di tecnologie e processi per implementare l'autenticazione a più fattori e la crittografia per i dati a riposo e in transito.

(iii) I capi delle agenzie FCEB che non sono in grado di adottare completamente l'autenticazione a più fattori e la crittografia dei dati entro 180 giorni dalla data di questo ordine dovranno, alla fine del periodo di 180 giorni, fornire una motivazione scritta al Segretario della Patria Sicurezza tramite il direttore della CISA, il direttore dell'OMB e l'APNSA.

(e) Entro 90 giorni dalla data di questo ordine, il Segretario della Sicurezza Nazionale che agisce tramite il Direttore della CISA, in consultazione con il Procuratore Generale, il Direttore dell'FBI e l'Amministratore dei Servizi Generali che agisce tramite il Direttore della FedRAMP , stabilisce un quadro per collaborare alla sicurezza informatica e alle attività di risposta agli incidenti relative alla tecnologia cloud FCEB, al fine di garantire un'efficace condivisione delle informazioni tra le agenzie e tra le agenzie e i CSP.

(f) Entro 60 giorni dalla data del presente ordine, l'Amministratore dei servizi generali, in consultazione con il Direttore dell'OMB e i capi di altre agenzie come ritenuto appropriato dall'Amministratore dei servizi generali, inizierà la modernizzazione di FedRAMP entro:

(i) stabilire un programma di formazione per garantire che le agenzie siano adeguatamente formate e attrezzate per gestire le richieste FedRAMP e fornire accesso a materiali di formazione, inclusi video su richiesta;

(ii) migliorare la comunicazione con i CSP attraverso l'automazione e la standardizzazione dei messaggi in ogni fase dell'autorizzazione. Queste comunicazioni possono includere aggiornamenti di stato, requisiti per completare la fase corrente di un fornitore, passaggi successivi e punti di contatto per domande;

(iii) incorporare l'automazione in tutto il ciclo di vita di FedRAMP, inclusi valutazione, autorizzazione, monitoraggio continuo e conformità;

(iv) digitalizzare e semplificare la documentazione che i fornitori sono tenuti a completare, anche attraverso l'accessibilità in linea e moduli precompilati; e

(v) identificare i framework di conformità rilevanti, mappare tali framework sui requisiti nel processo di autorizzazione FedRAMP e consentire a tali framework di essere utilizzati come sostituti della parte pertinente del processo di autorizzazione, a seconda dei casi.

Sec. 4. Migliorare la sicurezza della catena di fornitura del software.

(a) La sicurezza del software utilizzato dal governo federale è vitale per la capacità del governo federale di svolgere le sue funzioni critiche. Lo sviluppo di software commerciale spesso manca di trasparenza, sufficiente attenzione alla capacità del software di resistere agli attacchi e controlli adeguati per prevenire la manomissione da parte di malintenzionati. È urgente implementare meccanismi più rigorosi e prevedibili per garantire che i prodotti funzionino in modo sicuro e come previsto. La sicurezza e l'integrità del "software critico" - software che esegue funzioni critiche per la fiducia (come fornire o richiedere privilegi di sistema elevati o accesso diretto alle risorse di rete e di elaborazione) - è una preoccupazione particolare. Di conseguenza, il governo federale deve intervenire per migliorare rapidamente la sicurezza e l'integrità della catena di fornitura del software,con una priorità nell'affrontare il software critico.

(b) Entro 30 giorni dalla data di questo ordine, il Segretario del Commercio che agisce tramite il

Direttore del NIST solleciterà il contributo del Governo Federale, del settore privato, del mondo accademico e di altri attori appropriati per identificare o sviluppare nuovi standard, strumenti, e le migliori pratiche per conformarsi agli standard, alle procedure o ai criteri di cui alla sottosezione (e) di questa sezione. Le linee guida devono includere criteri che possono essere utilizzati per valutare la sicurezza del software, includere criteri per valutare le pratiche di sicurezza degli sviluppatori e dei fornitori stessi e identificare strumenti o metodi innovativi per dimostrare la conformità con le pratiche sicure.

(c) Entro 180 giorni dalla data di questo ordine, il Direttore del NIST pubblicherà linee guida preliminari, basate sulle consultazioni descritte nella sottosezione (b) di questa sezione e attingendo ai documenti esistenti come possibile, per migliorare la sicurezza della catena di fornitura del software e soddisfare i requisiti di questa sezione.

(d) Entro 360 giorni dalla data di questo ordine, il Direttore del NIST pubblicherà linee guida aggiuntive che includono procedure per la revisione periodica e l'aggiornamento delle linee guida descritte nella sottosezione (c) di questa sezione.

(e) Entro 90 giorni dalla pubblicazione delle linee guida preliminari ai sensi della sottosezione (c) di questa sezione, il Segretario del Commercio che agisce tramite il Direttore del NIST, in consultazione con i capi delle agenzie che il Direttore del NIST ritiene opportuno, dovrà emettere linee guida per identificare le pratiche che migliorano la sicurezza della catena di fornitura del software. Tale guida può incorporare le linee guida pubblicate ai sensi delle sottosezioni (c) e (i) di questa sezione. Tale guida deve includere standard, procedure o criteri riguardanti:

(i) ambienti di sviluppo software sicuri, comprese azioni quali:

(A) utilizzo di ambienti di compilazione separati dal punto di vista amministrativo;

(B) verifica dei rapporti di fiducia;

(C) stabilire l'autenticazione multifattoriale basata sul rischio e l'accesso condizionato in tutta l'azienda;

(D) documentare e ridurre al minimo le dipendenze dai prodotti aziendali che fanno parte degli ambienti utilizzati per sviluppare, creare e modificare il software;

(E) utilizzo della crittografia per i dati; e

(F) monitorare le operazioni e gli allarmi e rispondere ai tentativi e ai veri e propri incidenti informatici;

(ii) generare e, quando richiesto da un acquirente, fornire artefatti che dimostrino la conformità ai processi indicati nella sottosezione (e) (i) di questa sezione;

(iii) impiegando strumenti automatizzati, o processi comparabili, per mantenere catene di approvvigionamento di codice sorgente affidabili, garantendo in tal modo l'integrità del codice;

(iv) l'utilizzo di strumenti automatizzati o processi comparabili che verificano la presenza di vulnerabilità note e potenziali e le risolvono, che devono funzionare regolarmente o almeno prima del rilascio del prodotto, della versione o dell'aggiornamento;

(v) fornire, quando richiesto da un acquirente, artefatti dell'esecuzione degli strumenti e dei processi descritti nella sottosezione (e) (iii) e (iv) di questa sezione, e rendere disponibili al pubblico informazioni di sintesi al completamento di queste azioni, a includere una descrizione sintetica dei rischi valutati e mitigati;

(vi) mantenere dati accurati e aggiornati, provenienza (cioè origine) del codice o dei componenti del software e controlli sui componenti, strumenti e servizi del software interni e di terze parti presenti nei processi di sviluppo del software e svolgere audit e applicazione di questi controlli su base ricorrente;

(vii) fornire a un acquirente una distinta base software (SBOM) per ciascun prodotto direttamente o pubblicandola su un sito Web pubblico;

(viii) partecipare a un programma di divulgazione delle vulnerabilità che include un processo di segnalazione e divulgazione;

(ix) attestare la conformità a pratiche di sviluppo software sicuro; e

(x) garantire e attestare, per quanto possibile, l'integrità e la provenienza del software open

source utilizzato all'interno di qualsiasi parte di un prodotto.

(f) Entro 60 giorni dalla data del presente ordine, il Segretario del Commercio, in coordinamento con il Segretario aggiunto per le comunicazioni e l'informazione e l'Amministratore dell'amministrazione nazionale delle telecomunicazioni e dell'informazione, pubblicherà gli elementi minimi per un SBOM.

(g) Entro 45 giorni dalla data di questo ordine, il Segretario del Commercio, che agisce tramite il Direttore del NIST, in consultazione con il Segretario della Difesa che agisce tramite il Direttore della NSA, il Segretario della Sicurezza Nazionale che agisce tramite il Direttore del La CISA, il Direttore dell'OMB e il Direttore dell'intelligence nazionale, pubblicheranno una definizione del termine "software critico" da includere nella guida emessa ai sensi della sottosezione (e) di questa sezione. Tale definizione riflette il livello di privilegio o accesso richiesto per il funzionamento, l'integrazione e le dipendenze con altri software, l'accesso diretto alle risorse di rete e informatiche, le prestazioni di una funzione critica per la fiducia e il potenziale di danno se compromesso.

(h) Entro 30 giorni dalla pubblicazione della definizione richiesta dalla sottosezione (g) di questa sezione, il Segretario della Sicurezza Nazionale che agisce tramite il Direttore della CISA, in consultazione con il Segretario del Commercio che agisce tramite il Direttore del NIST, identificherà e mettere a disposizione delle agenzie un elenco di categorie di software e prodotti software in uso o nel processo di acquisizione che soddisfano la definizione di software critico rilasciata ai sensi della sottosezione (g) di questa sezione.

(i) Entro 60 giorni dalla data di questo ordine, il Segretario del Commercio che agisce tramite il Direttore del NIST, in consultazione con il Segretario della Sicurezza Nazionale che agisce tramite il Direttore della CISA e con il Direttore dell'OMB, pubblicherà le linee guida che delineano la sicurezza misure per il software critico come definito nella sottosezione (g) di questa sezione, inclusa l'applicazione di pratiche di privilegio minimo, segmentazione della rete e configurazione appropriata.

(j) Entro 30 giorni dall'emissione della guida descritta nella sottosezione (i) di questa sezione, il Direttore dell'OMB che agisce tramite l'Amministratore dell'Ufficio del governo elettronico all'interno dell'OMB dovrà adottare le misure appropriate per richiedere che le agenzie si conformino a tali linee guida .

(k) Entro 30 giorni dall'emissione delle linee guida descritte nella sottosezione (e) di questa sezione, il Direttore dell'OMB che agisce tramite l'Amministratore dell'Ufficio del governo elettronico all'interno dell'OMB dovrà adottare le misure appropriate per richiedere che le agenzie rispettino tali linee guida con rispetto al software acquistato dopo la data di questo ordine.

(l) Le agenzie possono richiedere un'estensione per soddisfare i requisiti emessi ai sensi della sottosezione (k) di questa sezione. Qualsiasi richiesta di questo tipo sarà esaminata dal Direttore dell'OMB caso per caso e solo se accompagnata da un piano per soddisfare i requisiti sottostanti. Il Direttore dell'OMB fornirà trimestralmente una relazione all'APNSA che identifichi e spieghi tutte le estensioni concesse.

(m) Le agenzie possono richiedere una deroga a qualsiasi requisito emesso ai sensi della sottosezione (k) di questa sezione. Le deroghe devono essere considerate dal Direttore dell'OMB, in consultazione con l'APNSA, caso per caso, e devono essere concesse solo in circostanze eccezionali e per una durata limitata, e solo se esiste un piano di accompagnamento per mitigare qualsiasi potenziale rischi.

(n) Entro 1 anno dalla data di questo ordine, il Segretario della Sicurezza Nazionale, in consultazione con il Segretario della Difesa, il Procuratore Generale, il Direttore dell'OMB e l'Amministratore dell'Office of Electronic Government all'interno dell'OMB, raccomanderà alla lingua del contratto del Consiglio FAR che richiede ai fornitori di software disponibile per l'acquisto da parte delle agenzie di rispettare e attestare di conformarsi a qualsiasi requisito emesso ai sensi delle sottosezioni da (g) a (k) di questa sezione.

(o) Dopo aver ricevuto le raccomandazioni descritte nella sottosezione (n) di questa sezione, il Consiglio FAR rivedrà le raccomandazioni e, come appropriato e in conformità con la legge

applicabile, modificherà il FAR.

(p) A seguito dell'emissione di qualsiasi regola finale che modifica il FAR come descritto nella sottosezione (o) di questa sezione, le agenzie devono, come appropriato e in conformità con la legge applicabile, rimuovere i prodotti software che non soddisfano i requisiti del FAR modificato da tutti consegna a tempo indeterminato contratti di quantità indefinita; Programmi di approvvigionamento federale; Contratti di acquisizione a livello di governo federale; Contratti di acquisto globali; e contratti di aggiudicazione multipli.

(q) Il Direttore di OMB, che agisce tramite l'Amministratore dell'Office of Electronic Government all'interno di OMB, richiederà alle agenzie che impiegano software sviluppato e acquistato prima della data di questo ordine (software legacy) di conformarsi a qualsiasi requisito emesso ai sensi della sottosezione (k) della presente sezione o per fornire un piano che delinei le azioni per rimediare o soddisfare tali requisiti e richiederà inoltre alle agenzie che richiedono il rinnovo dei contratti software, incluso il software legacy, di conformarsi a qualsiasi requisito emesso ai sensi della sottosezione (k) di questa sezione , a meno che non venga concessa un'estensione o una deroga in conformità con il comma (l) o (m) di questa sezione.

(r) Entro 60 giorni dalla data di questo ordine, il Segretario del Commercio che agisce tramite il Direttore del NIST, in consultazione con il Segretario della Difesa che agisce tramite il Direttore della NSA, pubblicherà le linee guida che raccomandano gli standard minimi per i il codice sorgente del software, inclusa l'identificazione dei tipi consigliati di test manuali o automatici (come strumenti di revisione del codice, analisi statica e dinamica, strumenti di composizione del software e test di penetrazione).

(s) Il Segretario del Commercio che agisce tramite il Direttore del NIST, in coordinamento con i rappresentanti di altre agenzie come il Direttore del NIST ritiene appropriato, avvierà programmi pilota informati dai programmi esistenti di etichettatura dei prodotti di consumo per educare il pubblico sulle capacità di sicurezza di Internet dispositivi IoT (-of-Things) e pratiche di sviluppo software e deve considerare modi per incentivare produttori e sviluppatori a partecipare a questi programmi.

(t) Entro 270 giorni dalla data di questo ordine, il Segretario del Commercio che agisce tramite il Direttore del NIST, in coordinamento con il Presidente della Commissione Federale per il Commercio (FTC) e rappresentanti di altre agenzie come il Direttore del NIST ritiene appropriato, identifica i criteri di cibersicurezza IoT per un programma di etichettatura dei consumatori e valuta se tale programma di etichettatura dei consumatori può essere gestito in combinazione con o modellato su programmi governativi esistenti simili conformi alla legge applicabile. I criteri devono riflettere livelli sempre più completi di prove e valutazioni a cui un prodotto può essere stato sottoposto e devono utilizzare o essere compatibili con i sistemi di etichettatura esistenti che i produttori utilizzano per informare i consumatori sulla sicurezza dei loro prodotti. Il Direttore del NIST esaminerà tutte le informazioni pertinenti,etichettatura e programmi di incentivazione e utilizzare le migliori pratiche. Questa revisione si concentrerà sulla facilità d'uso per i consumatori e sulla determinazione delle misure che possono essere prese per massimizzare la partecipazione del produttore.

(u) Entro 270 giorni dalla data di questo ordine, il Segretario del Commercio che agisce tramite il Direttore del NIST, in coordinamento con il Presidente della FTC e rappresentanti di altre agenzie come il Direttore del NIST ritiene appropriato, identificherà lo sviluppo sicuro del software pratiche o criteri per un programma di etichettatura di software per consumatori e deve considerare se tale programma di etichettatura di software per consumatori può essere utilizzato in combinazione con o modellato su programmi governativi esistenti simili, in conformità con la legge applicabile. I criteri devono riflettere un livello di base di pratiche sicure e, se possibile, devono riflettere livelli sempre più completi di test e valutazione a cui un prodotto può essere stato sottoposto. Il Direttore del NIST esaminerà tutte le informazioni pertinenti, l'etichettatura e i programmi di incentivi, impiegherà le migliori pratiche,e identificare, modificare o sviluppare un'etichetta consigliata o, se possibile, un sistema di classificazione della sicurezza del software a più livelli. Questa revisione si concentrerà

sulla facilità d'uso per i consumatori e sulla determinazione delle misure che possono essere prese per massimizzare la partecipazione.

(v) Questi programmi pilota devono essere condotti in modo coerente con la circolare OMB A-119 e la pubblicazione speciale NIST 2000-02 (Considerazioni sulla valutazione della conformità per le agenzie federali).

(w) Entro 1 anno dalla data di questo ordine, il Direttore del NIST condurrà una revisione dei programmi pilota, si consulterà con il settore privato e le agenzie competenti per valutare l'efficacia dei programmi, determinare quali miglioramenti possono essere fatti in futuro e inviare un rapporto di riepilogo all'APNSA.

(x) Entro 1 anno dalla data di questo ordine, il Segretario del Commercio, in consultazione con i capi di altre agenzie come il Segretario del Commercio ritenga opportuno, fornirà al Presidente, attraverso l'APNSA, un rapporto che esamina i progressi fatto in questa sezione e delinea i passaggi aggiuntivi necessari per proteggere la catena di fornitura del software.

Sec. 5. Istituire un comitato di revisione della sicurezza informatica.

(a) Il Segretario per la sicurezza interna, in consultazione con il Procuratore generale, istituirà il Comitato di revisione della sicurezza informatica (Consiglio), ai sensi della sezione 871 dell'Homeland Security Act del 2002 (6 USC 451).

(b) Il Consiglio esaminerà e valuterà, in relazione a incidenti informatici significativi (come definiti dalla Direttiva sulla politica presidenziale 41 del 26 luglio 2016 (Coordinamento degli incidenti informatici degli Stati Uniti) (PPD 41)) che interessano i sistemi informatici di FCEB o sistemi non federali , attività delle minacce, vulnerabilità, attività di mitigazione e risposte delle agenzie.

(c) Il Segretario della Sicurezza Nazionale convoca il Consiglio a seguito di un incidente informatico significativo che ha innescato l'istituzione di un Gruppo di coordinamento unificato Cyber (UCG) come previsto dalla sezione V (B) (2) della PPD-41; in qualsiasi momento secondo le istruzioni del Presidente che agisce tramite l'APNSA; o in qualsiasi momento il Segretario della Sicurezza Nazionale lo ritenga necessario.

(d) La revisione iniziale del Consiglio si riferirà alle attività cibernetiche che hanno portato alla creazione di un UCG nel dicembre 2020 e il Consiglio, entro 90 giorni dalla costituzione del Consiglio, fornirà raccomandazioni al Segretario della Sicurezza Nazionale per migliorare la sicurezza informatica e gli incidenti pratiche di risposta, come delineato nella sottosezione (i) di questa sezione.

(e) I membri del Consiglio includeranno funzionari federali e rappresentanti di enti del settore privato. Il Consiglio comprenderà rappresentanti del Dipartimento della Difesa, del Dipartimento di Giustizia, della CISA, della NSA e dell'FBI, nonché rappresentanti dei fornitori di sicurezza informatica o software appropriati del settore privato, secondo quanto stabilito dal Segretario della Sicurezza Nazionale. Un rappresentante dell'OMB parteciperà alle attività del consiglio quando un incidente in esame coinvolge i sistemi informativi di FCEB, come stabilito dal segretario della sicurezza nazionale. Il Segretario della Sicurezza Interna può invitare la partecipazione di altri, caso per caso, a seconda della natura dell'incidente in esame.

(f) Il Segretario della Sicurezza Nazionale designerà ogni due anni un presidente e un vicepresidente del consiglio tra i membri del consiglio, per includere un membro federale e un membro del settore privato.

(g) Il Comitato protegge le informazioni sensibili delle forze dell'ordine, operative, commerciali e altre informazioni riservate che sono state condivise con esso, in conformità con la legge applicabile.

(h) Il Segretario per la sicurezza interna fornirà al Presidente tramite l'APNSA qualsiasi consiglio, informazione o raccomandazione del Consiglio per migliorare la sicurezza informatica e le pratiche e la politica di risposta agli incidenti al termine della sua revisione di un incidente applicabile.

(i) Entro 30 giorni dal completamento della revisione iniziale descritta nella sottosezione (d) di questa sezione, il Segretario della Sicurezza Nazionale fornirà al Presidente attraverso l'APNSA le raccomandazioni del Consiglio basate sulla revisione iniziale. Tali raccomandazioni descrivono:

(i) le lacune identificate e le opzioni per la composizione o le autorità del Consiglio;

(ii) missione, ambito e responsabilità proposti dal Consiglio;

(iii) criteri di ammissibilità all'adesione per i rappresentanti del settore privato;

(iv) struttura di governance del consiglio, inclusa l'interazione con il ramo esecutivo e l'ufficio esecutivo del presidente;

(v) soglie e criteri per i tipi di incidenti informatici da valutare;

(vi) fonti di informazioni che dovrebbero essere messe a disposizione del Consiglio, coerentemente con la legge e la politica applicabili;

(vii) un approccio per proteggere le informazioni fornite al Consiglio e garantire la cooperazione delle persone e delle entità statunitensi interessate ai fini della revisione degli incidenti da parte del Consiglio; e

(viii) considerazioni amministrative e di bilancio richieste per il funzionamento del Consiglio.

(j) Il Segretario della Sicurezza Nazionale, in consultazione con il Procuratore Generale e l'APNSA, esaminerà le raccomandazioni fornite al Presidente tramite l'APNSA ai sensi della sottosezione (i) di questa sezione e prenderà le misure necessarie per attuarle.

(k) Salvo diversa indicazione del Presidente, il Segretario della Sicurezza Interna estenderà la vita del Consiglio ogni 2 anni come ritenuto appropriato dal Segretario della Sicurezza Nazionale, ai sensi della sezione 871 della Legge sulla Sicurezza Nazionale del 2002.

Sec. 6. Standardizzazione del playbook del governo federale per la risposta alle vulnerabilità e agli incidenti della sicurezza informatica.

(a) La vulnerabilità della sicurezza informatica e le procedure di risposta agli incidenti attualmente utilizzate per identificare, riparare e recuperare da vulnerabilità e incidenti che interessano i loro sistemi variano tra le agenzie, ostacolando la capacità delle agenzie principali di analizzare le vulnerabilità e gli incidenti in modo più completo tra le agenzie. I processi di risposta standardizzati garantiscono una catalogazione più coordinata e centralizzata degli incidenti e il monitoraggio dei progressi delle agenzie verso risposte di successo.

(b) Entro 120 giorni dalla data di questo ordine, il Segretario della sicurezza interna che agisce tramite il Direttore della CISA, in consultazione con il Direttore dell'OMB, il Consiglio dei funzionari federali per l'informazione e il Consiglio federale per la sicurezza delle informazioni, e in il coordinamento con il Segretario della Difesa che agisce tramite il Direttore della NSA, il Procuratore generale e il Direttore dell'intelligence nazionale, svilupperà una serie standard di procedure operative (playbook) da utilizzare nella pianificazione e conduzione di una vulnerabilità della sicurezza informatica e attività di risposta agli incidenti rispetto dei sistemi informativi FCEB. Il playbook deve:

(i) incorporare tutti gli standard NIST appropriati;

(ii) essere utilizzato dalle Agenzie FCEB; e

(iii) articolare il progresso e il completamento attraverso tutte le fasi di una risposta a un incidente, consentendo al contempo flessibilità in modo che possa essere utilizzato a supporto di varie attività di risposta.

(c) Il Direttore dell'OMB emetterà una guida sull'uso da parte dell'agenzia del playbook.

(d) Le agenzie con vulnerabilità alla sicurezza informatica o procedure di risposta agli incidenti che si discostano dal playbook possono utilizzare tali procedure solo dopo aver consultato il direttore dell'OMB e l'APNSA e aver dimostrato che queste procedure soddisfano o superano gli standard proposti nel playbook.

(e) Il Direttore della CISA, in consultazione con il Direttore della NSA, rivedrà e aggiornerà annualmente il playbook e fornirà informazioni al Direttore dell'OMB per incorporarle negli aggiornamenti delle linee guida.

(f) Per garantire la completezza delle attività di risposta agli incidenti e creare fiducia che gli attori informatici non autorizzati non abbiano più accesso ai sistemi informativi FCEB, il playbook stabilisce, in conformità con la legge applicabile, un requisito che il direttore della CISA riveda e convalidi l'incidente delle agenzie FCEB risultati della risposta e della riparazione al completamento della risposta all'incidente da parte di un'agenzia. Il direttore della CISA può raccomandare l'uso di un'altra agenzia o di un team di risposta agli incidenti di terze parti, a seconda dei casi.

(g) Per garantire una comprensione comune degli incidenti informatici e dello stato di sicurezza informatica di un'agenzia, il playbook definisce i termini chiave e utilizza tali termini coerentemente con qualsiasi definizione statutaria di tali termini, per quanto possibile, fornendo in tal modo un lessico condiviso tra le agenzie utilizzando il playbook.

Sec. 7. Miglioramento del rilevamento delle vulnerabilità della sicurezza informatica e degli incidenti sulle reti del governo federale.

(a) Il governo federale impiegherà tutte le risorse e le autorità appropriate per massimizzare il rilevamento precoce delle vulnerabilità e degli incidenti della sicurezza informatica sulle sue reti. Questo approccio includerà l'aumento della visibilità del governo federale e del rilevamento delle vulnerabilità della sicurezza informatica e delle minacce alle reti di agenzie al fine di rafforzare gli sforzi di sicurezza informatica del governo federale.

(b) Le agenzie FCEB implementeranno un'iniziativa Endpoint Detection and Response (EDR) per supportare il rilevamento proattivo degli incidenti di sicurezza informatica all'interno dell'infrastruttura del governo federale, la caccia attiva, il contenimento e la riparazione e la risposta agli incidenti.

(c) Entro 30 giorni dalla data di questo ordine, il Segretario della Sicurezza Nazionale che agisce tramite il Direttore della CISA fornirà al Direttore dell'OMB raccomandazioni sulle opzioni per l'attuazione di un'iniziativa EDR, in posizione centrale per supportare la visibilità a livello di host, l'attribuzione e risposta in merito ai sistemi informativi FCEB.

(d) Entro 90 giorni dalla ricezione delle raccomandazioni descritte nella sottosezione (c) di questa sezione, il Direttore dell'OMB, in consultazione con il Segretario della Sicurezza Nazionale, emetterà i requisiti per le Agenzie FCEB per adottare approcci EDR a livello di Governo Federale. Tali requisiti supportano la capacità del Segretario del Segretario nazionale, che agisce tramite il Direttore della CISA, di impegnarsi in attività di caccia, rilevamento e risposta informatici.

(e) Il Direttore dell'OMB lavorerà con il Segretario della Sicurezza Nazionale e i capi delle agenzie per garantire che le agenzie abbiano risorse adeguate per conformarsi ai requisiti emessi ai sensi della sottosezione (d) di questa sezione.

(f) La difesa dei sistemi informativi FCEB richiede che il Segretario per la sicurezza interna, che agisce tramite il Direttore della CISA, abbia accesso ai dati dell'agenzia che sono rilevanti per un'analisi delle minacce e delle vulnerabilità, nonché per scopi di valutazione e caccia alle minacce. Entro 75 giorni dalla data del presente ordine, le agenzie devono stabilire o aggiornare Memoranda of Agreement (MOA) con CISA per il Programma di diagnostica e mitigazione continua per garantire che i dati a livello di oggetto, come definito nel MOA, siano disponibili e accessibili a CISA, coerenti con la legge applicabile.

(g) Entro 45 giorni dalla data di questo ordine, il Direttore della NSA in qualità di Responsabile nazionale per i sistemi di sicurezza nazionale (Responsabile nazionale) raccomanderà al Segretario della Difesa, al Direttore dell'intelligence nazionale e al Comitato per la sicurezza nazionale Systems (CNSS) azioni appropriate per migliorare il rilevamento degli incidenti informatici che interessano i sistemi di sicurezza nazionale, nella misura consentita dalla legge applicabile, comprese le raccomandazioni sugli approcci EDR e se tali misure debbano essere gestite dalle agenzie o attraverso un servizio centralizzato di interesse comune fornito dal Direttore nazionale.

(h) Entro 90 giorni dalla data di questo ordine, il Segretario della Difesa, il Direttore dell'intelligence nazionale e il CNSS rivedranno le raccomandazioni presentate ai sensi della

sottosezione (g) di questa sezione e, se appropriato, stabiliranno le politiche che le attuano. raccomandazioni, coerenti con la legge applicabile.

(i) Entro 90 giorni dalla data di questo ordine, il Direttore della CISA fornirà al Direttore dell'OMB e dell'APNSA un rapporto che descrive come le autorità concesse ai sensi della sezione 1705 del diritto pubblico 116-283, per condurre attività di caccia alle minacce su Le reti FCEB senza previa autorizzazione delle agenzie sono in fase di implementazione. Questo rapporto raccomanda anche le procedure per garantire che i sistemi mission-critical non vengano interrotti, le procedure per la notifica ai proprietari dei sistemi di sistemi governativi vulnerabili e la gamma di tecniche che possono essere utilizzate durante il test dei sistemi informativi FCEB. Il direttore della CISA fornirà rapporti trimestrali all'APNSA e al direttore dell'OMB in merito alle azioni intraprese ai sensi della sezione 1705 del diritto pubblico 116-283.

(j) Per garantire l'allineamento tra le direttive DODIN (Department of Defense Information Network) e le direttive FCEB Information Systems, il Segretario della Difesa e il Segretario della Sicurezza Nazionale, in consultazione con il Direttore dell'OMB, dovranno:

(i) entro 60 giorni dal la data di questo ordine, stabilire le procedure per il Dipartimento della Difesa e il Dipartimento per la Sicurezza Interna per condividere immediatamente tra loro gli Ordini di Risposta agli Incidenti del Dipartimento della Difesa o le Direttive di Emergenza del Dipartimento per la Sicurezza Nazionale e le Direttive Operative Vincolanti applicabili alle rispettive reti di informazione;

(ii) valutare se adottare eventuali indicazioni contenute in un Ordine o Direttiva emanate dall'altra Direzione, coerenti con la normativa in materia di condivisione delle informazioni classificate; e

(iii) entro 7 giorni dalla ricezione della notifica di un Ordine o Direttiva emessa in conformità alle procedure stabilite nella sottosezione (j) (i) di questa sezione, informare l'APNSA e l'amministratore dell'Ufficio del governo elettronico all'interno dell'OMB della valutazione descritta nella sottosezione (j) (ii) della presente sezione, inclusa la determinazione dell'opportunità di adottare le linee guida emesse dall'altro Dipartimento, la motivazione di tale determinazione e una tempistica per l'applicazione della direttiva, se applicabile.

Sec. 8. Miglioramento delle capacità investigative e di riparazione del governo federale.

(a) Le informazioni provenienti dai registri di rete e di sistema sui sistemi informativi federali (sia per i sistemi locali che per le connessioni ospitate da terze parti, come i CSP) sono inestimabili sia per scopi di indagine che di riparazione. È essenziale che le agenzie e i loro fornitori di servizi IT raccolgano e conservino tali dati e, quando necessario per affrontare un incidente informatico sui sistemi informativi FCEB, li forniscano su richiesta al Segretario della Sicurezza Nazionale tramite il Direttore della CISA e all'FBI, coerentemente con la legge applicabile.

(b) Entro 14 giorni dalla data di questo ordine, il Segretario della Sicurezza Nazionale, in consultazione con il Procuratore Generale e l'Amministratore dell'Office of Electronic Government all'interno dell'OMB, fornirà al Direttore dell'OMB raccomandazioni sui requisiti per la registrazione degli eventi e conservare altri dati rilevanti all'interno dei sistemi e delle reti di un'agenzia. Tali raccomandazioni devono includere i tipi di log da conservare, i periodi di tempo per conservare i log e altri dati pertinenti, i periodi di tempo per le agenzie per consentire la registrazione raccomandata e i requisiti di sicurezza e come proteggere i log. I log devono essere protetti con metodi crittografici per garantire l'integrità una volta raccolti e periodicamente verificati contro gli hash durante la loro conservazione.I dati devono essere conservati in modo coerente con tutte le leggi e i regolamenti sulla privacy applicabili. Tali raccomandazioni devono essere prese in considerazione anche dal Consiglio FAR in sede di promulgazione delle regole ai sensi della sezione 2 del presente decreto.

(c) Entro 90 giorni dalla ricezione delle raccomandazioni descritte nella sottosezione (b) di questa sezione, il Direttore dell'OMB, in consultazione con il Segretario del Commercio e il Segretario della Sicurezza Nazionale, formulerà le politiche affinché le agenzie stabiliscano i requisiti per il

disboscamento, conservazione dei registri e gestione dei registri, che assicurano l'accesso centralizzato e la visibilità per il centro operativo di sicurezza di più alto livello di ciascuna agenzia.

(d) Il Direttore dell'OMB lavorerà con i responsabili delle agenzie per garantire che le agenzie dispongano di risorse adeguate per conformarsi ai requisiti identificati nella sottosezione (c) di questa sezione.

(e) Per affrontare rischi o incidenti informatici, inclusi potenziali rischi o incidenti informatici, le raccomandazioni proposte emesse ai sensi della sottosezione (b) di questa sezione devono includere requisiti per garantire che, su richiesta, le agenzie forniscano registri al Segretario della Sicurezza Nazionale attraverso il Direttore della CISA e dell'FBI, in conformità con la legge applicabile. Questi requisiti dovrebbero essere progettati per consentire alle agenzie di condividere le informazioni di registro, se necessario e appropriato, con altre agenzie federali per rischi o incidenti informatici.

Sec. 9. Sistemi di sicurezza nazionale.

(a) Entro 60 giorni dalla data di questo ordine, il Segretario della Difesa che agisce tramite il Direttore nazionale, in coordinamento con il Direttore dell'intelligence nazionale e del CNSS, e in consultazione con l'APNSA, adotterà i requisiti dei Sistemi di sicurezza nazionale che sono equivalente o superiore ai requisiti di sicurezza informatica stabiliti in questo ordine che altrimenti non sono applicabili ai sistemi di sicurezza nazionale. Tali requisiti possono prevedere eccezioni in circostanze rese necessarie da esigenze di missione uniche. Tali requisiti devono essere codificati in un memorandum sulla sicurezza nazionale (NSM). Fino al momento in cui viene emesso il NSM, i programmi, gli standard o i requisiti stabiliti ai sensi del presente ordine non si applicano ai sistemi di sicurezza nazionale.

(b) Nulla in questo ordine altererà l'autorità del Responsabile nazionale rispetto ai Sistemi di sicurezza nazionale come definito nella Direttiva sulla sicurezza nazionale 42 del 5 luglio 1990 (Politica nazionale per la sicurezza delle telecomunicazioni e dei sistemi informativi di sicurezza nazionale) (NSD- 42). La rete FCEB continuerà ad essere sotto l'autorità del Segretario della Sicurezza Nazionale che agisce attraverso il Direttore della CISA.

Sec. 10. Definizioni. Ai fini del presente ordine:

(a) il termine "agenzia" ha il significato ad esso attribuito in 44 USC 3502.

(b) il termine "relazione di fiducia di controllo" indica una relazione concordata tra due o più elementi del sistema che è regolata in base a criteri di interazione, comportamento e risultati sicuri relativi alla protezione delle risorse.

(c) il termine "incidente informatico" ha il significato attribuito a un "incidente" in 44 USC 3552 (b) (2).

(d) il termine "Agenzie del ramo esecutivo civile federale" o "Agenzie FCEB" include tutte le agenzie ad eccezione del Dipartimento della difesa e le agenzie della Comunità di intelligence.

(e) il termine "Sistemi informativi del ramo esecutivo civile federale" o "Sistemi informativi FCEB" indica quei sistemi informativi gestiti dalle agenzie del ramo esecutivo civile federale, ma esclude i sistemi di sicurezza nazionale.

(f) il termine "Sistemi informativi federali" indica un sistema informativo utilizzato o gestito da un'agenzia o da un appaltatore di un'agenzia o da un'altra organizzazione per conto di un'agenzia, inclusi i sistemi informativi FCEB e i sistemi di sicurezza nazionale.

(g) il termine "Intelligence Community" o "IC" ha il significato ad esso attribuito in 50 USC 3003 (4).

(h) il termine "Sistemi di sicurezza nazionale" indica i sistemi di informazione come definiti in 44 USC 3552 (b) (6), 3553 (e) (2) e 3553 (e) (3).

i) il termine "registri" indica le registrazioni degli eventi che si verificano all'interno dei sistemi e delle reti di un'organizzazione. I registri sono composti da voci di registro e ciascuna voce contiene

informazioni relative a un evento specifico che si è verificato all'interno di un sistema o di una rete.

(j) il termine "Distinta materiali del software" o "SBOM" indica un record formale contenente i dettagli e le relazioni della catena di fornitura dei vari componenti utilizzati nella creazione del software. Sviluppatori e fornitori di software spesso creano prodotti assemblando componenti software commerciali e open source esistenti. Lo SBOM enumera questi componenti in un prodotto. È analogo a un elenco di ingredienti sugli imballaggi alimentari. Uno SBOM è utile a coloro che sviluppano o producono software, a coloro che selezionano o acquistano software e a coloro che utilizzano software. Gli sviluppatori utilizzano spesso componenti software open source e di terze parti disponibili per creare un prodotto; uno SBOM consente al costruttore di assicurarsi che quei componenti siano aggiornati e di rispondere rapidamente alle nuove vulnerabilità. Gli acquirenti possono utilizzare uno SBOM per eseguire analisi di vulnerabilità o licenze,entrambi possono essere utilizzati per valutare il rischio in un prodotto. Coloro che utilizzano software possono utilizzare SBOM per determinare rapidamente e facilmente se sono a rischio potenziale di una vulnerabilità scoperta di recente. Un formato SBOM ampiamente utilizzato e leggibile dalla macchina consente maggiori vantaggi grazie all'automazione e all'integrazione degli strumenti. Gli SBOM acquisiscono un valore maggiore se archiviati collettivamente in un repository che può essere facilmente interrogato da altre applicazioni e sistemi. Comprendere la catena di fornitura del software, ottenere un SBOM e utilizzarlo per analizzare le vulnerabilità note sono fondamentali nella gestione del rischio.Il formato SBOM leggibile dalla macchina consente maggiori vantaggi grazie all'automazione e all'integrazione degli strumenti. Gli SBOM acquisiscono un valore maggiore se archiviati collettivamente in un repository che può essere facilmente interrogato da altre applicazioni e sistemi. Comprendere la catena di fornitura del software, ottenere un SBOM e utilizzarlo per analizzare le vulnerabilità note sono fondamentali nella gestione del rischio.Il formato SBOM leggibile dalla macchina consente maggiori vantaggi grazie all'automazione e all'integrazione degli strumenti. Gli SBOM acquisiscono un valore maggiore se archiviati collettivamente in un repository che può essere facilmente interrogato da altre applicazioni e sistemi. Comprendere la catena di fornitura del software, ottenere un SBOM e utilizzarlo per analizzare le vulnerabilità note sono fondamentali nella gestione del rischio.

(k) il termine "Architettura Zero Trust" indica un modello di sicurezza, un insieme di principi di progettazione del sistema e una strategia coordinata di sicurezza informatica e gestione del sistema basata sul riconoscimento che le minacce esistono sia all'interno che all'esterno dei confini della rete tradizionale. Il modello di sicurezza Zero Trust elimina la fiducia implicita in qualsiasi elemento, nodo o servizio e richiede invece una verifica continua del quadro operativo tramite informazioni in tempo reale da più fonti per determinare l'accesso e altre risposte del sistema. In sostanza, un'architettura Zero Trust consente agli utenti l'accesso completo ma solo al minimo indispensabile per svolgere il proprio lavoro. Se un dispositivo è compromesso, zero trust può garantire che il danno sia contenuto. Il modello di sicurezza Zero Trust Architecture presume che una violazione sia inevitabile o probabilmente si sia già verificata,quindi limita costantemente l'accesso solo a ciò che è necessario e cerca attività anomale o dannose. Zero Trust Architecture incorpora un monitoraggio completo della sicurezza; controlli di accesso granulari basati sul rischio; e automazione della sicurezza del sistema in modo coordinato in tutti gli aspetti dell'infrastruttura al fine di concentrarsi sulla protezione dei dati in tempo reale all'interno di un ambiente di minaccia dinamico. Questo modello di sicurezza incentrato sui dati consente di applicare il concetto di accesso con privilegi minimi per ogni decisione di accesso, dove le risposte alle domande su chi, cosa, quando, dove e come sono fondamentali per consentire o negare in modo appropriato l'accesso alle risorse basate sulla combinazione di sever.controlli di accesso granulari basati sul rischio; e automazione della sicurezza del sistema in modo coordinato in tutti gli aspetti dell'infrastruttura al fine di concentrarsi sulla protezione dei dati in tempo reale all'interno di un ambiente di minaccia dinamico. Questo modello di sicurezza incentrato sui dati consente di applicare il concetto di accesso con privilegi minimi per ogni decisione di accesso, dove le risposte alle domande su chi, cosa, quando, dove e come sono fondamentali per consentire o negare in modo appropriato l'accesso alle risorse basate

sulla combinazione di sever.controlli di accesso granulari basati sul rischio; e automazione della sicurezza del sistema in modo coordinato in tutti gli aspetti dell'infrastruttura al fine di concentrarsi sulla protezione dei dati in tempo reale all'interno di un ambiente di minaccia dinamico. Questo modello di sicurezza incentrato sui dati consente di applicare il concetto di accesso con privilegi minimi per ogni decisione di accesso, dove le risposte alle domande su chi, cosa, quando, dove e come sono fondamentali per consentire o negare in modo appropriato l'accesso alle risorse basate sulla combinazione di sever.dove le risposte alle domande su chi, cosa, quando, dove e come sono fondamentali per consentire o negare in modo appropriato l'accesso alle risorse in base alla combinazione di sever.dove le risposte alle domande su chi, cosa, quando, dove e come sono fondamentali per consentire o negare in modo appropriato l'accesso alle risorse in base alla combinazione di sever.

Sec. 11. Disposizioni generali.

(a) Alla nomina del Direttore informatico nazionale (NCD) e all'istituzione del relativo Ufficio all'interno dell'Ufficio esecutivo del Presidente, ai sensi della sezione 1752 della legge pubblica 116-283, parti di questo ordine possono essere modificate per consentire il NCD per eseguire pienamente i suoi doveri e responsabilità.

(b) Nulla in questo ordine deve essere interpretato in modo da pregiudicare o in altro modo influenzare:

(i) l'autorità concessa per legge a un dipartimento o agenzia esecutiva, o al suo capo; o

(ii) le funzioni del Direttore dell'Ufficio di gestione e bilancio relative a proposte di bilancio, amministrative o legislative.

(c) Questo ordine deve essere eseguito in modo coerente con la legge applicabile e subordinatamente alla disponibilità di stanziamenti.

(d) Questo ordine non ha lo scopo di creare e non crea alcun diritto o vantaggio, sostanziale o procedurale, applicabile per legge o secondo equità da qualsiasi parte contro gli Stati Uniti, i suoi dipartimenti, agenzie o entità, i suoi funzionari, dipendenti , o agenti o qualsiasi altra persona.

(e) Nulla in questo ordine conferisce l'autorità di interferire con o di dirigere un'indagine penale o di sicurezza nazionale, un'operazione di arresto, perquisizione, sequestro o interruzione o di alterare una restrizione legale che richiede a un'agenzia di proteggere le informazioni apprese nel corso di un indagini penali o di sicurezza nazionale.

JOSEPH R. BIDEN JR.

THE WHITE HOUSE,
12 maggio 2021