



National Cyber
Security Centre
a part of GCHQ



Australian Government
Australian Signals Directorate

ACSC Australian
Cyber Security
Centre



Communications
Security Establishment

Centre de la sécurité
des télécommunications

Canadian Centre
for Cyber Security

Centre canadien
pour la cybersécurité



National Cyber Security Centre
Ministry of Justice and Security

certnz



National Cyber
Security Centre
PART OF THE GCSB



Fetu'una'iga o le Paleni i lamatiaga mai
osofaiga i luga o initaneti: Manatu
faavae (Principles) ma auala e faatino
ai (Approaches) i le Security-by-Design and-
Default.

Lomiga: 13 o Aperila, 2023

Cybersecurity and Infrastructure Security Agency

NSA | FBI | ACSC | NCSC-UK | CCCS | BSI | NCSC-NL | CERT NZ | NCSC-NZ

Disclaimer: O lenei pepa ua faailogaina TLP.CLEAR. E lē o faatapula'aina lona faailoaina. E mafai ona faaoga e i latou na maua mai ai ia faamatalaga le TLP: CLEAR pe afai o faamatalaga o loo faaveaia o loo aafia ai sina lamatiaga laitiiti pe leai foi ole faaoga seseina. Ina ia o gatasi ma tulafono e tatau ona apalai iai mo le faalauiloaina lautele. Fua agai i tulafono faavae o mataupu tau copyright, o faamatalaga tau TLP: CLEAR e mafai ona tufatufaina e aunoa ma se faasaina. Mo nisi faamatalaga silasila i le the Traffic Light Protocol, silasila i le <http://www.cisa.gov/tlp/>

Mea o loo Aofia.

<i>Mea o loo Aofia</i>	2
Aotelega: Vulnerable by Design.....	3
<i>Secure-by-Design</i>	5
<i>Secure-by-Default</i>	6
Fautuaga Mo ē Fausia Polokalame Komipiuta	7
<i>Manatu faavae mo Polokalame tau komipiuta ma Puipuiga</i>	7
<i>Taumafaiga faatatau i le Secure-by-Design</i>	9
<i>Taumafaiga mo le Secure-by-Default</i>	12
Hardening vs loosening guides (Ta’iala).....	14
Recommendations for Customers (Fautuaga Mo Tagata Faatau).....	14
Disclaimer	15
Resources (Mea E Faatino Ai Galuega)	16

AOTELEGA: VULNERABLE BY DESIGN

O le faa tekonoosi (technology) ua toeitiiti aofia i vaega uma o le soifuaga i aso taitasi. O polokalame fa’aaoga i le initaneti ua koneti agai i isi systems e sili atu ona t̄ua ma iai o latou aafiaga tuusa’o i le tulaga tau le tamaoaiga, le tuputupua’e aemaise le soifua maloloina, mai lava i le puleaina o tulaga tau le tagata lava ia faasolo atu i le tausiga tau le soifua maloloina. O se tasi o faataitaiga, o cyber breaches po o osofaiga i luga o le initaneti ua oo ai ina l̄ faataunuuina ai nisi o taotoga i maota gasegase ma le fetuunaiga o le tausiga o gasegase i tulaga faavaomalo. O tulaga faa tekonoosi e l̄ malupuipua ma faigofie ona lamatia i systems (Insecure technology and vulnerabilities) e t̄ua tele e ono valaaulia ane ai ma ni osofaiga ogaoga i luga o le initaneti ma oo ai ina iai i se tulaga ogaoga ma lamatiaga i le saogalemu¹.

E aupito sili lava i le taimi nei le t̄ua o le faia e technology manufacturers (tagata latou te fausia faiga faatekonolosi), o le Secure-by-Design ma le Secure-by Default, o le taulaiga aut̄ lea o le faatulagana o oloa ma le faiga o galuega faalatele. O nisi o le aufaipisinisi ua tulaga lelei a latou laasaga ua faia i le aveina i luma o le auaunaga i tulaga tau polokalame tau komiputa (software) o loo faaaogaina, e ui o isi o loo fai si faatuai. O loo unaia malosi e ofisa ua tuufaatasia nei tusitusiga (authoring agency) le unaia o soo se technology manufacturer ina ia fausia a latou oloa i se auala e taofia ai tagata faatau mai le fai ma o latou faatino siaki ma faatonutonu tulaga tau le faatinoina o le auaunaga i a latou systems ina ia faaititiia ai osofaiga i luga o le initaneti. O loo unaia manufacturers ina ia o latou umia le faaleleia o tulaga tau puipuiga ma le iuga o ia tulaga mo a latou tagata faatau. Mai lona talafaasolopito sa faalagolago ai lava technology manufacturers i le faaleleia o mea sa iai i ni tulaga lamatia ina ua tuuina atu oloa i tagata faatau ma manaomia ai tagata faatau ina ia faatino ia mea faaleleia mai a latou lava tupe. Sei vagana ua faa aofia atu le faiga lea o le Secure-by-Design ona gausia lea o le faataamilosaga lea o le fausia o se oloa ma toe tau faalelei.

Ina ia ausia lea tulaga maualuga i tulaga tau le puipuiga, ua unaia ai nei e ofisa o loo tuufaatasia nei tusitusiga, manufacturers ina ia ave le faamuamua i le faa aofia ai o le puipuiga mo le oloa, o se vaega taua lea e tatau ona ausia mo le vave o le oo o oloa i le maketi. Ao alu pea aso o le a mafai e le ‘au Inisinia ona o latou amataina se faiga maut̄ o le a faaaofia ai lava ma le itu tau le puipuiga i le taimi e fausia ai se oloa ma l̄ toe tele ai ni gaioiga e faia i le faatumauiina o lona lelei.

Ile toe tomanatu ai i lenei faiga, ua toe faamalosia mai ai e le luni a Europa le t̄ua o le puipuiga o se oloa. I lalo ole [Cyber-Resilience Act](#), o le faamanino lelei o manufacturers e tatau ona o latou faia se faiga e malupuipua ai manufacturers mai le faalauiloina o a latou oloa o loo iai i ni tulaga lamatia i luga o le maketi.

¹ O loo amanaia e ofisa o loo tuufaatasia lenei tusitusiga ole faaaogaina o le upu “saogalemu” e tele ona uiga mae fua lava i le faaaogaina o loo faaaoga ai. Mo le faamoemoe o lenei taiala, o le upu ‘safety’ poo le saogalemu o le a faauiga tonu i le siitia o le tulaga tau le puipuiga i mataupu faa tekonoosi e puipui ai paaga mai osofaiga ogaoga i luga o le initaneti.

Ina ia fausia se lumanai saogalemu mo faiga faatekonolosi ma oloa o loo aafia ai mo tagata faatau , ua unaia ai e ofisa o loo tuu faatasia nei tusitusiga, le toe fetuunaiga e manufacturers o a latou design ma polokalame faalautele ia faataga ai na’o oloa a le Secure-by-Design and-Default e lafoina i tagata faatau. O oloa ua Secure-by-Design o oloa ia o loo faa ogatotonugalemu ai le puipuiga o le tagata faatau a le kamupani i ana taulaiga (goals), ae lē na o se isi vaega o le auaunaga. O oloa e Secure-by Design e amata i le taulaiga lea ao lei amata ona faalautele. O oloa e Secure-by-Default, o oloa ia o loo saogalemu e faaoga pe a tatalaina mai le pusa e aunoa ma se toe tau faia iai o nisi fetuunaiga poo nisi tau faaopoopo e totogi.

A tuu faatasi, o nisi o nei faiga tāua e lua o le a aveesea ai se vaega tele o le avega ole nofo mautinoa i manufacturers ma faaitiitia ai avanoa e ono aafia ai i latou i ni tulaga tau le puipuiga e mafua mai i mea e lē o lelei ona faatulaga, le vave ona faaleleia o mea faaleagaina ma isi lava faaletonu taatele.

O le Cybersecurity and Infrastructure Security Agency (CISA), le National Security Agency (NSA), Federal Bureau of Investigation (FBI) ma isi paaga faavaomalo latou te saunia fautuaga i lenei taiala², o se faafanua mo technology manufacturers e faamautu ai le puipuiga mo a latou oloa.

- Australian Cyber Security Centre (ACSC)
- Canadian Centre for Cyber Security (CCCS)
- United Kingdom’s National Cyber Security Centre (NCSC-UK)
- Germany’s Federal Office for Information Security (BSI)
- Netherlands’ National Cyber Security Centre (NCSC-NL)
- Computer Emergency Response Team New Zealand (CERT NZ) and New Zealand’s National Cyber Security Centre (NCSC-NZ).

O loo amanaia e ofisa ua tuu faatasia lenei tusitusiga le sao na faia e nisi o paaga e toatele mai le private sector i le unaia o le security-by design ma le security-by-default. O lenei oloa ua faia e fuafua i le agai i luma o ni faatalanoaga faavaomalo e faatatau i mataupu o loo ave iai le faamuamua, inivesi ma faaiuga talafeagai e ausia ai se lumanai e saogalemu ai faiga faatekonolosi, mautū, ma tulaga ese foi i le design and default. I le tau faai’ui’uga ua sailia ai e ofisa ua tuu faatasia nei tusitusiga, ni finagalo faaalua i le oloa aemaise mai vaega o loo fia silafia le oloa ma fuafua e faatulaga se faasologa o faatalanoaga ia sana atili faaleleia ai , faafou ma faamaioio lelei le agai i luma o le tatou taiala ina ia ausia ai taulaiga faasoa.

Mo nisi faamatalaga le tāua o le saogalemu o le oloa, silasila le tusitusiga i le CISA, [O le Tau o le lē Malu Puipuia o Tekonolosi ma O ā mea e Mafai Ona Tatou Faia i ai \(The Cost of Unsafe Technology and What We Can Do About It\)](#).

² O lea ua faaigoaina “authoring agencies”

Secure-by-Design

O le Secure-by Design o lona uiga o oloa tau tekonoosi ua fausia i se auala ua malupuipua ai mai osofaiga ogaoga ua mafai ona saofia atu i luga o le initaneti agai i lau masini, data ma isi vaega o loo koneti uma ifo. O i latou e fausia polokalame mo komipiuta (software manufacturers) e tatau ona o latou faia se iloilogia (risk assessment) e iloa ai ma faitau ai faamata'u ia e faia mai i le initaneti agai i systems aupito tāua (critical systems), ma faa aofia ai ni puipuga mo oloa ma mea o loo fausia mai ai (product blueprint).

O faamatalaga faa tekonoosi ua malupuipua (Secure IT), fuafuaga faalautele ma isi faasologa o puipuga e faaigoa o puipuga loloto e fautuaina foi le faia ina ia taofia ai gaioiga lē lelei e ono aafia ai systems pe maua ai foi ma le avanoa e ulufale ai e aunoa ma se faatagana ma silasila i faamaumauga maaleale. O ofisa o loo latou tuu faatasia lenei tusitusiga ua o latou fautuaina manufacturers ina ia fa'aaoga se faiga (tailored threat model) i le taimi e faalautele ai se oloa ina ia silasila ai loa i soo se ituaiga faamata'u e faia i se system ma sailia tonu ai lona fa'aogaina.

O ofisa ua tuu faatasia lenei tusitusiga (authoring agency) ua o latou unaia manufacturers ina ia fai se faiga e tuu faatasia uma ai elemeni e malupuipua ai a latou oloa ma platforms. O le faalauteleina o le Secure-by Design e manaomia ai le inivesi iai o alaga'oa (resources) e i latou e faia polokalame tau komipiuta (software manufacturers) i vaega eseese o le faatulagana o le oloa atoa ai ma isi vaega faalautele e le mafai ona toe faapipii atu iai mulimuli ane. E manaomia ai se taitaiga malosi mai faauluuluga o le pisinisi lea latou te faia ia polokalame ina ia faamuamua le puipuga ae le faapea ua nao se tasi faiga faa tekonoosi. O lea galulue so'oso'otau'au i le va o taitai o pisinisi ma 'au o loo galulue i faiga faatekonosi e amata mai i uluai taimi o le faatulagana o se oloa ma lona faalauteleina, agai atu i le faaogaina e paaga ma lona faatumaui. Ua unaia manufacturers ina ia faia faaiuga faigata tau fefaatauaiga (hard trade-offs) ma inivesi, e aofia ai ma faaiuga e le mafai ona iloa mai e tagata faatau a le kamupani e pei o fetuunaiga e faia i gagana tau polokalame e aveesea ai le iai i se tulaga lamatia i lona aotelega. E tatau ona o latou faamuamua mea o loo aofia i se oloa, o lona faiga ma le faatinoina o mea faigaluega e puipui ai tagata faatau nai lo le silasila i mea o loo aofia i se oloa e foliga e manaia i le vaai ae atili tele ai le avanoa e osofaia mai ai.

E leai se tali mautū se tasi e faamuta ai le faifaipia mai o faamata'u ogaoga a i latou e faia mai osofaiga (cyber actors) e fa'aaoga mai ai tulaga maaleale o faiga faatekonosi ma o oloa ua faailoga

Secure-by-Design o le a fa'aauau pea foi ona mafatia i tulaga maaleale ia peitai o se vaega tele lava o tulaga maaleale e mafua mai i sina vaega itiiti lava o loo faapogai mai ai. E tatau i manufacturers ona o latou faalautele ni faasinoala ia o gatasi ai a latou oloa ma faiga a le Secure-by-Design ia mautinoa e faatoa agai ese mai lea faiga pe a oo ini mataupu ua tulaga ese.

O ofisa ua tuufaatasia lenei tusitusiga latou te fia faailoa o le umiaina o le faaiuga o itu tau le puipuiga mo tagata faatau ma le faamautuina o le ituaiga maua luga lea o le puipuiga mo tagata faatau, e mafai ai ona siitia a latou tau mo le faalauteleina o le auunaga. Ui i lea, o le faiga o le inivesi i le Secure-by-Design ao faalautele nisi oloa fou tau tekonolosi ma faamautu nisi oloa o iai nei, o le a ono faaleleia ai le tulaga tau le puipuiga a tagata faatau ma faaitiitia ai le ono iai i se tulaga e osofaia ai. O manatu faavae (principles) o le Secure-by-Design e le gata ina faamalosi ai le tulaga tau le puipuiga mo tagata faatau ma le talafaasolopito o le brand poo le ituaiga oloa o loo faaoga, ae faaitiitia ai foi ma tau mo le faatumauiina o tulaga lelei (maintenance) ma mea toe faaleleia mo manufacturers mo se taimi umi.

O le vaega o fautuaga, (Recommendations for Software Manufacturers section) o loo lisi atu i lalo ua saunia atu ai se lisi o faiga faalautele e manaomia ona faia i se oloa ma faiga faavae mo manufacturers e silasila iai.

Secure-by-Default

O le Secure-by-Default o lona uiga o oloa o loo lavasaia tulaga lamatia e aafia ai ile taimi e amata faaoga ai, e aunoa ma nisi totogi faaopoopo. O oloa ia e puipuia mai faamata'u aupito ogaoga ma tulaga maaleale e aunoa ma le toe iai o nisi laasaga e faia e tagata e faaogaina a latou oloa ina ia malupuipua ai latou. O oloa a le Secure-by-Default ua faaata lava ina ia matuai malamalama paaga afai latou te agai ese mai mai faiga tau le puipuiga ua maea faatulaga, o le a o latou faatupulaia ai le ono iai o oloa ia i se tulaga e ono osofaia ai sei vagana ua o latou faatino nisi faiga fa'aopoopo e faatonutonu ai nisi mea e ono totogi atu.

- O le Secure Configuration o se faufauga mautū e tatau ona avea ma vaega amata autu. O oloa a le Secure-by-Default e otomeki ona o latou faataga faiga taua tau le puipuiga e faatonutonu ai enterprises mai osofaiga a cyber actors, aemaise o le tuuina o le faatagana (in this case, ability) e faaoga ai ma soona faufau ai tulaga tau le puipuiga e aunoa ma nisi totogi faaopoopo.
- O le lavelave o faufauga mautū e le tatau ona avea o se faafitauli a le tagata faatau. E masani lava ona tele galuega faaopopo mo le aufaigaluega i le IT ona o le matafaioi i tulaga tau le puipuiga ma

tiute fai, o le ala lea e iu ai ina itiiti le taimi e malamalama ma faatino ai tulaga tau le puipuiga ma fetuunaiga e manaomia ia faaleleia ai pea le tulaga tau le puipuiga mai osofaiga i le initaneti. O le matuai faaaogaina o le tulaga lea i faufauga mautu mo oloa ma le faamautuina o le “default path”, e mafai e manufacturers ona fesoasoani i a latou paaga e ala i le faamautuina lelei o loo fausia, tufatufaina ma faaaogaina lelei oloa ia o gatasi ma aiaiga a le Secure-by-Default.

O i latou e gaosia oloa a le Secure-by-Default latou te le toe tuuina nisi tau faaopoopo mo le faatinoina o nisi tulaga tau le puipuiga sa faaopoopoina i se oloa. Peitai latou te faa aofia uma ia mea ile uluai oloa e tai pei ona aofia ai ma fusipau o nofoa i soo se taavale fou. O le tulaga tau le puipuiga e le o se tulaga taugata peitai e latalata i le tulaga e tatau ai mo soo se tagata faatau ona faatalitalia e aunoa ma nisi feutanaiga e toe faia pe o nisi foi totogi faaopopo.

RECOMMENDATIONS FOR SOFTWARE MANUFACTURERS (FAUTUAGA MO Ē FAUSIA POLOKALAME KOMIPIUTA)

O lenei taiala e saunia atu ai fautuaga mo manufacturers mo le faalauteleina o se faafanua tusitusia i le faatinoina ma le faamautuina o tulaga tau le puipuiga i faamatalaga faatekonolosi. O loo fautuaina e ofisa o loo tuufaatasia lenei tusitusiga le faia e software manufacturers o nisi o auala e pei ona faataatia atu i le vaega pito i lalo ina ia o latou umia ai le tulaga e oo iai puipuiga mo tagata faatau e ala i manatu faavae o le Secure-by-Design and Default.

Software Product Security Principles (Manatu faavae mo Polokalame tau komipiuta ma Puipuiga)

O loo unaia technology manufacturers poo i latou e fausia faiga faatekonolosi ina ia fai se faiga e taulai i ai le faamuamua i le tulaga tau le puipuiga mo le software. Ua faalautele e ofisa o loo tuufaatasia lenei tusitusiga i le vaega pito i lalo, ni manatu faavae se tolu e limataitaiina ai software manufacturers i le fausiaina o puipuiga mo le software i totonu o a latou fuafuaga faataatitia ao lei faalauteleina, faufau ma lafoina a latou oloa.

1. E le tatau ona pa’ū tasi le avega o le puipuiga i le tagata faatau. O Software manufacturers e tatau ona o latou umia le tulaga e oo iai faatauga a a latou paaga ma faataamilo agai iai a latou oloa.
2. Ia taofimau faiga sa’o ma faamaoni. E tatau i software manufacturers ona mitamita ia i latou lava ona o le kilivaina o ni oloa saogalemu ma malupuipua, ae le gata i lea o le faeseina mai o

latou mai se vaega tele o le komiuniti o manufacturers, fua i luga o lo latou agavaa e faatino ai lea tulaga. E ono aofia ai le faasoaina o faamatalaga sa o latou a’oina mai mai a latou tagata faatau e pei o le fa’aaogaina o nisi o faiga malolosi mo le faamaoniaina (authentication mechanisms). E aofia ai foi ma se tautinoga malosi e faamautu ai o loo ua maea faamautu ma o loo sa’o faamaumauga e faatatau i fautuaga i tulaga maaleale ma nisi lamatiaga taatele ma le faailoaina (CVE). Peitai, ia faaeteete i le faaosoosoga ina ia faitau le CVE o se tasi o tulaga le lelei (negative metric) ona o nisi o numera ia o se faailo o se faailoga tau le soifua maloloina ma faataitaiga i komiuniti.

3. Fausia faatulagana ma taitaiga tau faalapopotoga ina ia ausia ai nei moemitiga. E ui e taua tele le tomai e faatatau i le autu o le mataupu i tulaga tau le puipuiga o se oloa, o ofisa sinia lava oi latou ia e faia le faaiuga mo le faatinoina o nei suiga i se faalapopotoga. O mea ua taula’i iai (commitments) e faia i tulaga mauualuluga (executive level) mo software manufacturers e ave ai le faamuamua i le puipuiga, o se vaega taua i le puipuiga o se oloa e manaomia ai le faalateleina o faiga faapaaga ma tagata faatau a se faalapopotoga ina ia malamalama:
 - a. O le taiala i le fa’aaogaina o se oloa faatasi ai ma le faataitaiga o faamata’u (tailored threat model).
 - b. Fuafuaga mo le faatinoina o mea faatonutonu tau le puipuiga ia o gatasi ma manatu faavae o le Secure-by-Default.
 - c. O faiga ua faatulaga mo le tuuina o alagaoa (resources) fua ile telē o le kamupani ma le faatagana e suia ai faiga faalatele na sau ai e ala ile faaaogaina o faiga a le Secure-by-Design.
 - d. Le manaoga ina ia faatumaui pea se laina matala mo fesootaiga mo manatu fa’aalia e le gata i totonu ae o fafo atu foi o le kamupani (faataitaiga, manatu faaalia o tagata faigaluega ma paaga) e faatatau i tulaga tau le puipuiga o se oloa. O le puipuiga o le software o se tasi lea o vaega e ao ona ave iai le faamamafa i faatalanoaga i totonu lava ia o le kamupani (faataitaiga, all-hands or brown bags) aemaise o le maketiina atu o oloa i fafo ma le auai ai o tagata faatau.
 - e. O le fua po o tulaga lelei o le tuuina atu o oloa i tagata faatau. O le a fia malamalama sui sinia o le kamupani poo gafea tonu o loo fesoasoani ai inivesi ua faia i le Security

by design and defaults i nisi o ana paaga, e ala i le faatuai o le faatinoina o galuega faaleleia i le itu tau le puipuiga, faaitiitia o faaletonu i le taimi na faufau ai le oloa ma faaitiitia lamatiaga.

Ina ia faataga manatu faavae ia e tolu, e tatau i manufacturers ona silasila i nisi o taumafaiga mo le faataamilosaga o a latou faiga faalatele.

Ia faia fonotaga faifaiepea ma sui sinia o kamupani ina ia unai ai le taua o le Secure-by-Design ma le Secure-by-Default i totonu o le faalapopotoga. O faiga faavae ma auala e ao ona faatulaga ina ia faamanuia ai 'au o loo latou fausia oloa (production team) ma mulimulitai i manatu faavae ia, e mafai foi ona aofia atu ai ma faailoga mo le faatinoina o auala aupito lelei mo puipuiga o software po o ni faamanuiaga foi mo le siitia o tulaga i galuega (promotion criteria).

Faatino galuega i le li'o o le tāua o le puipuiga o le software mo le manuia o le pisinisi. Mo se faataitaiga, silasila ile faa ō gatasi o le “software security leader” poo le software security team lea latou te feagai ma mataupu tau pisinisi ma faamatalaga faatekonolosi, ina ia fesootai sa’o lava tulaga tau le puipuiga o softwares ma le amiotonu o manufacturers. O manufacturers e ao ona o latou faamautinoa o loo ise tulaga lelei ma tutoatasi le iloiloga o tulaga tau le puipuiga i le oloa atoa ai foi ma polokalame toe faatulaga (evaluation programme) mo a latou oSoftware Bill of Materialsloa.

Ia fa’aaoga le tailored threat model i le taimi e faalatele ai se oloa ina ia ave ai le faamuamua i vaega aupito taua ma oloa e tetele aafiaga. O threats models latou te iloilo tulaga patino i se oloa ma faataga development teams ('au latou te faalateleina se oloa) ina ia faamalosi oloa. I lona faaiuga, o tagata taitai sinia e ao ona o latou faamautinoa i 'au poo teams nei o latou e nafa ma matafaioi o le kilivaina o ni oloa saogalemu, o se tasi lea o elemeni autu o se oloa i sona tulaga atoatoa ma lelei.

Taumafaiga faatatau i le Secure-by-Design

O le faavaa mo le Secure Software Development (SSDF) e igoa foi o le National Institute of Standards and Technology (NIST) [SP 800-218](#), ose faiga mautu e maua lona faatulagana i tulaga tau le puipuiga e mafai ona faa aofia mai i totonu o vaega eseese o le faalateleina o se oloa (SDLC), software development lifecycle. O le mulimu'ita'i i le faiga lea e mafai ai ona fesoasoani i software producers ia faigofie ona aoga i le sailiga ma le aveesea o tulaga maaleale i se polokalame poo le software, fetuunai aafiaga e ono tulai mai i le faaogaina o itu maaleale ia ma agai sa’o loa i le faapogai ole faaletonu ia alofia ai le toe tulai mai i le lumanai.

E unaia e ofisa o loo feagai ma le tuufaatasia o lenei tusitusiga, le fa’aaoga o taumafaiga a le Secure-by-Design, e aofia ai ma manatu faavae o loo taua ai faiga a le SSDF. E ao foi i software manufacturers ona faalautele se faafanua tusitusia ina ia aofia ai nisi faiga faaopoopo a le Secure-by-Design. O loo tusia atu i lalo se lisi o nisi o ni faataitaiga aupito sili tau faafanua e iai ma ata:

- Memory Safe Programming languages (SSDF PW.6.1): Faamuamua le fa’aaoga o le memory safe language i soo se taimi e manaomia ai. O loo amanaia e ofisa o loo tuufaatasia lenei tusitusiga, e iai isi fetuunaiga i tulaga faapea (memory specific mitigations) e pei o le tuatusi ma lona faataatiaga (ASLR), control-flow integrity (CFI), fuzzing (ose polokalame otomeki e tuuina ni mea le talafeagai) e fesoasoani lea mo polokalame fausia mai faiga faatekonolosi tuai, ae o le a le lava lea e ta’ua ai o se Secure-by-design ona e le lava le itu tau le puipuiga e taofia ai le fa’aaogaina sese. O nisi faataitaiga o le modern memory safe language e aofia ai le C#, Rust, Ruby, Java, Go ma le Swift. Faitau i le NSA’S memory safety [information sheet](#) mo nisi faamatalaga,
- Secure Hardware Foundation:
E aofia ai tulaga faatatau i le fausiaina (architectural features) e mafai ai ona malupuipua le memory e pei ona faamatala mai i le Capability Hardware Enhanced Risc Instructions (CHERI) lea e mafai ona latou faalautele isi ituaiga faatonuga tau hardware-Set Architectures (ISAs). Mo nisi faamatalaga asiasi i le [CHERI webpage](#) i le University of Cambridge.
- Secure Software Components (SSDF PW 4.1): Ia maua ma faamautuina polokalame malupuipua (faataitaiga, software libraries, o modules, middleware, frameworks) mai pisinisi, soo se tagata, ma isi pati e aofia i le faalautelea ina ia faamautu ai le tulaga lelei o puipuiga i oloa a tagata faatau e aofia ai polokalame (consumer software products).
- Web template frameworks (SSDF PW 5.1): Fa’aaoga faavaa mai le upega tafailagi lea latou te faaogaina tulaga otomeki e alofia ai ni osofaiga i luga o le upega tafailagi e pei o le cross-site scripting.
- Parameterized queries (SSDF PW 5.1) Ia fa’aaoga parameterized queries nai lo le user input in queries ina ia alofia ai ni osofaiga mai le SQL injection.
- Static and dynamic application security testing (SAST/DAST)(SSDF PW 7.2, PW.8.2):
Fa’aaoga meafaigaluega ia e faatusatusa ai oloa ma mea na aumai ai atoa ai ma lona fa’aaogaina ina ia mafai ai ona iloagofie ni mea sese e ono aofia ai. O nei meafaigaluega e mafai ona kava ai ma mataupu e aofia ai le le vaaia lelei o le memory mai ni faaletonu e ono aafia ai (faataitaiga, unescaped user input leading to SQL injection). O meafaigaluega a le SAST ma le DAST e tatau ona faigofie ona fa’aaoga faatasi e faia ai se suesuega ia faamautu ai e utagia e oloa le ituaiga manaoga manaomia tau le puipuiga. Afai ae iai ni faaletonu e alia’e, e ao i manufacturers ona faatino loa le root-cause analysis po o le faiga e iloa tonu ai le faapogai o le faaletonu ina ia iloa ai tulaga maaleale o iai.
- Code review (SSDF PW.7.1, PW.7.2):

Faamalosia e faamautinoa ole code sa tuuina i totonu o oloa o loo alu sa’o lava i le iloiloga o loo faia (peer review) e isi developers ina ia faamautinoa ai le tulaga maualuga ma lelei e iai.

- [Software Bill of Materials³ \(SBOM\)](#) (SSDF PS.3.2, PW.4.1):
Faa aofia le faatuina o le SBOM ina ia maua ai se vaaiga i totonu o le seti o polokalame (software) lea e fa’aaoga i oloa.
- Vulnerability disclosure programs (SSDF RV.1.3):
Amata polokalame e faailoa ai tulaga maaleale o oloa e mafai ai ona faataga le au suesue i mataupu tau le puipuiga e lipotia tulaga maaleale ma ia maua foi le puipuiga faaletulafono a’o faatino lea galuega. O se vaega o lenei faiga e tatau ai i suppliers ona amata faagaioi ni auala ia mautinoa moni ai le faapogai autu o tulaga maaleale ua faailoa ane. O ia ituaiga auala e tatau ona aofia ai ma le faamautinoaina o loo fa’aaoga se faiga e pei o le Secure-by-Design pei ona faailoa atu i lenei pepa (po’o nisi foi auala e tali tutusa) e mafai ona o latou taofia le faalauiloaina o le tulaga maaleale.
- CVE completeness: (Common Vulnerabilities and Exposure) Faamautinoa o CVE (Tulaga Maaleale Taatele ma le Faailoaina) ua lomia o loo aofia ai ma o latou faapogai po o ni vaivaiga taatele i polokalame tau komipiuta. (CWE- Common Weakness Enumeration) ina ia faataga ai se suesuega auiliili o faapogai o tulaga tau le puipuiga i polokalame tau komipiuta. E ui o le faamautinoaina o lo’o sa’o ma mae’a CVE uma, e ono alu ai le taimi faaopoopo, ae e mafai ona faataga ai entities po’o totino eseese e maitau mai ni suiga po’o se faatau lega oni mea e penefiti uma ai manufacturers ma paaga. Mo nisi faamatalaga e faatatau i le faatonutonuina o tulaga maaleale, silasila ile taiala [CISA’s Stakeholder-specific SVCC](#).
- Defense-in-Depth: Faatulaga le infrastructure (mea o loo aofia ile siomaga) ina ia aua nei avea le iai o se tulaga e ono faaletonu ai se vaega se tasi o le puipuiga e avea ma ala e faaletonu atoa uma ai le system. Mo se faataitaiga ina ia faamautinoa o loo faatulaga lelei faamanuiaga e maua e le tagata na te faaaogaina le auaunaga aemaise o le faia o lisi o mea e faataga ona faaaoga, o le a faaititia ai aafiaga o se account ua faaletonu. Ae le gata i lea, ole faaaogaina o se faiga tau puipuiga i komipiuta (software sandboxing) o le a mafai ai ona faanofoesea ai se tulaga maaleale ma faaititia ai le ono faaletonu o se talosaga atoa.
- Satisfy Cyber Performance Goals (CPGs):
Faatulaga oloa e ausia faiga amata tau le puipuiga. O le [CISA’s Cybersecurity Performance Goals](#) o loo folasia atu ai se faiga faavae o ni tulaga tau le puipuiga mai osofaiga i luga o le initaneti, e ao ona faaaoga e faalapopotoga. Mo se faaopoopoga, mo nisi auala e faamalosi atili ai le tulaga o le faalapopotoga, silasila i le [UK’s Cyber Assessment Framework](#) lea latou te faaaogaina foi faiga e tali tutusa i le CISA’s ma CPGs- e pei o le le manaomiaina o le phishing-

³ O loo iloilo e nisi o ofisa o loo tuu faatasia lenei tusitusiga nisi auala ia faamautinoa ai le itu tau le puipuiga i le vaega e sapalaia polokalame tau komipiuta (software)

resistant multi-factor authentication mo tagata faigaluega uma ona e lē tatau ona vaaia o loo latou kilivaina oloa a le Secure-by-Design.

Ua maitauina e ofisa o loo tuufaatasia lenei tusitusiga o nei suiga o ni fetuunaiga taua tele i se tulaga o se faalapotopotoga. O le ala lea e ao ai ona faamuamua le latou faatomuaga e fua i luga o le tāua, lavelave ma aafiaga tau pisinisi. O nei faiga uma e mafai ona faailoa mo polokalame tau komipiuta ma faalatele ina ia aofia atu ai ma nisi mea faaopoopo ua fa’aaogaina faapea ma oloa. I le tele o mataupu o tulaga faigata ma lamatiaga o le tulaga o se oloa e ono afua ai se faiga faatopetope e fa’aaoga ia ituaiga faiga. I isi mataupu o faiga ia e mafai ona faailoa i ni systems tuai o komipiuta ma toe faafou mai lea taimi i lea taimi.

Taumaifaiga mo le Secure-by-Default

Faaopoopo atu i le faatinoina o le faiga o le Secure-by-Design ma lona faalateleina, ua fautuaina ai e ofisa o loo tuufaatasia lenei tusitusiga le ave o le faamuamua a software manufacturers i fetuunaiga ua faia i oloa a le Secure-by-Default. E tatau ona finau e faafou (update) oloa ina ia o gatasi ma ia ituaiga faiga pe a toe oomi le faamau e refresh ai. Mo se faataitaiga:

- Aveese passwords sa fai:

E le tatau ona aumai oloa faatasi ai ma passwords ia sa faatulaga ona o loo faasoaina faalauaitele. Ina ia aveesea passwords ia, e fautuaina e ofisa o loo tuufaatasia lenei tusitusiga le faatulaga e administrators o ni passwords malolosi i le taimi e faapipii ma amata faatulaga ai. Faamalosia le faia o le Multifactor Authentication ([MFA](#)) mo i latou e iai faamanuiaga i le fa’aaogaina. Matou te maitauina o le tele o le fa’aaogaina o le auaunaga e enterprises o loo faatonutonuina e administrators e le o malupuipua a latou accounts ile MFA. Pe afai o administrators nei o ni taulaiga maua luga, e tatau la ona faia le MFA opt out nai lo le opt in. Aemaise ai o le system e ao lava ona fai ma faamanatu le administrator ina ia lesitala i le MFA sei vagana ua o latou faatagaina le faaaogaina o le MFA i a latou accounts. O le taiala a Netherlands le NCSC o loo agai foi i le itu o loo iai le CISA’s, asiasi i le latou [Mature Authentication Factsheet](#) mo nisi faamatalaga faaopopo.

- Single sign-on (SSO):

Talosaga i faamatalaga faatekonolosi (IT) e ao ona faatino ai le faiga faatekonolosi o le single sign on fa’aaoga ai faiga fou nei e fa’aaoga tele e tagata. O faataitaiga e aofia ai le Security Assertion Markup Language (SAML) poo le OpenID Connect (OIDC). O lenei agavaa e mafai ona avanoa mai e aunoa ma se totogi.

- Secure Logging: Saunia i paaga se tulaga maua luga o audit logs poo faamaumauga o mea sa faatino i le system e aunoa ma se totogi faaopoopo. O audit logs e taua tele mo le mata’ituina ma tulituliloaina o ni tulaga faaletonu e ono tulai mai tau le puipuiga. E taua tele foi i le taimi o se sutesuega o se mataupu tau le puipuiga o loo masalomia pe ua faamaonia foi. Ia silasila i faiga

aupito lelei e pei ona saunia ane o se auala faigofie mo le tuufaatasia o faamatalaga tau le puipuiga ma systems o loo puleaina meafai (SIEM) ma le application programming interface (API) e fa'aaoga ai le ituaiga taimi o le (UTC), le ituaiga taimi e taua o le standard zone formatting atoa ai ma ituaiga tomai i le teuina o faamaumauga.

- **Software Authorization Profile:** O i latou e sapalaia polokalame tau komipiuta (software suppliers) e tatau ona o latou saunia ni fautuaga faataau i matafaioi faatagaina ma mea ua fa'aaogaina e fa'aaoga ai. E tatau i manufacturers ona faa aofia atu ma se lapataiga e mafai ona silasila ma logoina ai tagata faatau i se tulaga lamatia ua faateteleina pe afai ae o latou o ese mai mai tulaga faatagaina (profile authorization) o loo fautuaina atu. Mo se faataitaiga: o fomaini tau le soifua maloloina e mafai ona o latou silasila i faamaumauga o a latou gasegase, peitai o le tagata e faia bookings po o avanoa tau soifua maloloina, e itiiti le avanoa na te silasila ai i faamatalaga uma e manaomia e faatino ai le faiga o appointments.
- **Forward-looking security over backwards compatibility:** E masani lava ona faa aofia atu ma compatible-legacy features (po o ni vaega tuai tau komipiuta) ma masani ona toe fa'aaoga i oloa e ui e iai so latou lamatiaga i le tulaga tau le puipuiga o le oloa. Ia faamuamua le puipuiga i lo le backwards compatibility, ma ia faamallosia 'au o loo feagai ma le puipuiga ina ia aveese features po o ni vaega e le saogalemu tusa lava pe o le a mafua ai ona faatino ni suiga.
- **Track and reduce 'hardening guide size':** Faaitiitia le telē o taiala ua faia faapitoa mo le puipuia o tulaga faalilolilo o au systems (hardening guides) ua saunia mo oloa ma finau ina ia faamautinoa o le telē o le taiala o le a faaitiitia i se taimi pe afai foi e avanoa ane nisi ituaiga fou o lea ituaiga software. Tuufaatasi mea o loo aofia atu i le hardening guide, o le faufauga masani lea o lea oloa. E amanaia e ofisa o loo tuufaatasia lenei tusitusiga o hardening guides e pupuu e mafua mai i faiga faapaaga e fa'aaauu pea ma tagata faatau o loo iai ma e aofia ai ma taumafaiga mai nisi o le production teams, e aofia ai ma tomai a tagata e fa'aaogaina le auaunaga (UX).
- **Ia silasila i tulaga tau i le fa'aaogaina o le tomai o le tagata e fa'aaogaina le auaunaga i tulaga tau le puipuiga:** O soo se faatulagana fou i le system e faaopopo ai le avega po o le aofai o faamatalaga e mafai ona teuina e tagata e fa'aaogaina le auaunaga ma e tatau ona iloilo faatasi ma penefiti tau pisinisi o loo maua ane ai. E sili ai ona lē iai se setting: ae ia o le setting aupito i saogalemu e tatau ona tuufaatasi i le oloa. Afai e manaomia ona toe faufau, o le uluai filifiliga (default option) e tatau ona matua lautele lona saogalemu mai faamata'u taatele.

E amanaia e ofisa o loo tuufaatasia lenei tusitusiga, o nei suiga e ono iai ni o latou aafiaga i le faafaigaluegaina o lea software. O lea la, o le sao o tagata faatau e tūua tele i le faapaleniina o iloiloga tau galuega ma le puipuiga. E talitonu ofisa o loo tuufaatasia lenei tusitusiga ole faalauteleina o faafanua tusitusia ma le lagolago a sui sinia latou te faamuamua ia ituaiga manatu i oloa aupito taua a le faalapotopotoga, o le uluai laasaga lea i le se'e atu agai i le faalauteleina o ni software e saogalemu. E ui e tūua le sao o tagata faatau, ua silasila foi ofisa o loo tuufaatasia lenei tusitusiga i nisi o mataupu tūua ua iloa ai le lē mananao o tagata faatau pe lē mafai foi ona o latou taliaina ni tulaga ua faaleleia, pei ona masani ai aiaiga mautu tau sootaga (network protocols). E tūua mo manufacturers ina ia faia ni

incentives e uigā mo tagata faatau ina ia faatumauina ai pea ae lē o le faataga oi latou e tumau pea i se tulaga maaleale.

HARDENING VS LOOSENING GUIDES (TA’IALA)

O Hardening guides (taiala ia e puipui ai tulaga faalilolilo) e mafua mai i le lē lava o tulaga tau puipuiga mo oloa ma e tamau i totonu o le fausaga o se oloa mai lava i le amata mai o lona faalauteleaga. O le ala lea e mafai ai ona avea hardening guides o se faafanua mo i latou e faasagatau mai, latou te faasinosinomia ai ma fa’aaoga vaega o polokalame e lē o saogalemu. E taatele i le mau faalapopototoga le leiloa o hardening guides, ma o loo tuu ai ma le faufauga o a latou masini i se tulaga lē saogalemu. O se isi la ituaiga faataitaiga ua faaigoa o le loosening model e tatau ona suia ai hardening guides ma faamalamalama ai po o fea tonu suiga e tatau i users (tagata e fa’aaogaina le auaunaga) ona latou faia ma ia faamauina foi lamatiaga tau le puipuiga e feagai ma latou.

Ese mai i le faalauteleina o hardening guides e lisi mai ai oloa ma auala mo le faamautuina o le saogalemu, e fautuaina e ofisa o loo tuufaatasia lenei tusitusiga i latou o loo saunia polokalame ina ia faasee mai i le faiga lea o le Secure-by-Default e ala i le saunia o loosening guides.

O ia taiala la te faamatalaina lamatiaga o pisinisi i le faiga o faaiuga i mataupu i se gagana e manino ma faigofie ona malamalama ai, ma mafai ai ona siitia le silafia o faalapopototoga e uiga i lamatiaga mai osofaiga i luga o le initaneti. O Fefaatauiga tau le Puipuiga (Security Trade-offs) e ao ona faamautu mai e ofisa sinia a tagata faatau, faapaleni ai le tulaga tau le puipuiga ma isi mea e manaomia o le pisinisi.

RECOMMENDATIONS FOR CUSTOMERS (FAUTUAGA MO TAGATA FAATAU)

E fautuaina e ofisa o loo tuufaatasia lenei tusitusiga, faalapopototoga uma ina ia avea ma matafaioi a i latou o loo saunia faiga faatekonolosi, le feagai ma le puipuiga o oloa. O se vaega o lenei faiga ua fautuaina ai foi e ofisa o loo tuufaatasia lenei tusitusiga le faamuamua e ofisa silia o le faalapopototoga, o le taua o le faatauina o oloa a le Secure-by-Design ma le Secure-by-Default. E mafai ona faamalosia le tulaga lea e ala i le faia o ni faiga faavae e manaomia ai le vaega o le IT ia o latou asiasi le tulaga o iai le saogalemu o polokalame tau komipiuta ua saunia ae lei faatauina, ae le gata i lea o le faamalosia o le vaega a le IT ina ia toe tuutuu teisi i tua pe afai e manaomia. E tatau ona faamalosia le vaega o le IT ina ia o latou faalautele le faatulagana o le faiga o faatau e ave ai le faamamafa i le tāua o faiga ia o le Secure-by-Design ma le Secure-by-Default (e le gata i mea o loo faailoa atu i lenei pepa ae o isi o loo faaalutele e le faalapopotoga). Faaopoopo atu i lea, e ao ona lagolagoina le vaega a le IT e sui sinia o le Pulega i le taimi e faamalosia ai ia faatulagana i le faia o faaiuga mo faatauga.

O faaiuga e faia a le faalapopototoga e taliaina ai lamatiaga e aofia ai i oloa taitasi tau tekonolosi, e tatau ona faamauina aloaia ma ia ioeina e se sui sinia tau le pisinisi ma ia fai ma tuuina i le vasega o faatonu. O nisi auaunaga autu a le enterprise e lagolago ai le tulaga tau le puipuiga o se faalapopototoga e pei o le sootaga a le enterprise, tulaga faalilolilo o le enterprise ma ona avanoa i tulaga tau pulega, gaioiga fai i tulaga tau puipuiga ma le tali atu i luitau, e ao ona avea lea o ni agavaa

tāua tele tau pisinisi e faatupeina ina ia o gatasi ma lo latou tāua i le manuia o misiona a le faalapotopotoga. E ao i faalapotopotoga ona faalatele se fuafuaga e faaleleia atili ai ia agavaa ma faapaleni ai foi ma manufacturers o loo latou lagolagoina o faiga ia o le Secure-by-Design ma le Secure-by-Default.

I vaega e talafeagai ai, e ao i faalapotopotoga ona finau ina ia faia faiga faapaaga ma mafutaga ma a latou IT suppliers mautu. O ia ituaiga mafutaga e aofia ai le faatuatuaina i vaega e tele o le faalapotopotoga ma ia saunia foi auala mo le foia o faaletonu ma ia maitau mea e ave iai le faamuamua. O le puipuiga e tatau ona avea o se elemeni tāua tele o ia ituaiga mafutaga ma e tatau i faalapotopotoga ona finau ina ia faamalosia le tāua o faiga nei o le Secure-by-Design ma le Secure-by-Default i tulaga aloaia (faataitaiga-..., konekarate ma maliega ma vendors) ma isi vaega e le faamamaluina i le mafutaga. O faalapotopotoga e tatau ona o latou faatalitalia faiga sa’o mai i e saunia tulaga faatekonolosi e uiga i le tulaga o iai latou i le lotoifale faatasi ai ma le latou faafanua agai atu i le fa’aaogaina o le Secure-by-Design ma le Secure-by-Default.

Faaopopo atu i le ave o le faamuamua i le Security-by-Default i totonu o se faalapotopotoga, e ao i taitai tau le IT ona galulue faatasi ma tagata e mataituina le latou auaunaga, ina ia malamalama po o fea oloa ma auaunaga e aupito sili ona aofia ai ia ituaiga designs. O taitai ia e tatau ona tuufaatasi le latou talosaga ina ia fesoasoani i manufacturers e faamuamua a latou fuafuaga tau le puipuiga o loo loma ane. O le galulue faatasi, o le a fesoasoani ai tagata faatau i le saunia o ni sao uigā mo manufacturers ma ia fausia ai ni taumafaiga (incentives) mo i latou ia faamuamua ai lava le itu tau le puipuiga.

I le faapaleniina o cloud systems (kilivaina o auaunaga tau komipiuta), e tatau i faalapotopotoga ona faamautinoa o loo latou malamalama i le faasoaina o matafaioi (share responsibility model) ma i latou e sapalaia faiga faatekonolosi. O le mea lea, o faalapotopotoga e tatau ona iai la latou malamalamaaga i matafaioi a i latou e sapalaia matafaioi tau le puipuiga. E tatau i faalapotopotoga ona faamuamua cloud providers e faamaoni e faatatau i le tulaga o iai le latou itu tau le puipuiga, faatonutonuga o tulaga faalotoifale ma le agavaa e mafai ai ona ausia ona tiute ma matafaioi i lalo o le shared responsibility model.

DISCLAIMER

O le faamatalaga i lenei lipoti o loo ua saunia atu i le tulaga o iai nei mo le faamoemoe e faailoaina atu

faamatalaga. O le CISA ma ofisa o loo tuufaatasia lenei tusitusiga, latou te faatagaina ni oloa faapisinisi ma auaunaga, e aofia ai ma soo se mataupu tau suesuega. O soo se faamatalaga agai i ni totino faapisinisi patino po o ni oloa faapisinisi, faiga, ma auaunaga ma faailo, pe o se manufacturer po o se isi, e le mafai ona tuuina iai se faatagana, fautuaga pe o se faiga faaitu'au e le CISA ma ofisa o loo tuufaatasia lenei tusitusiga. O lenei pepa o se galuega fai faatasi a le CISA e le otomeki ona avea o se pepa faale-tulafono.

RESOURCES (MEA E FAATINO AI GALUEGA)

CISA

- [CISA's SBOM Guidance](#)
- [CISA's Cross-Sector Cybersecurity Performance Goals](#)
- [Guidelines on Technology Interoperability](#)
- [CISA and NIST's Defending Against Software Supply Chain Attacks](#)
- [The Cost of Unsafe Technology and What We Can Do About It | CISA](#)
- [Stop Passing the Buck on Cybersecurity: Why Companies Must Build Safety Into Tech Products \(foreignaffairs.com\)](#)
- [CISA's Stakeholder-Specific Vulnerability Categorization \(SSVC\) Guidance](#)
- [CISA's Phishing Resistant MFA Fact Sheets](#)
- [Cyber Guidance for Small Businesses | CISA](#)

NSA

- [NSA's Cybersecurity Information Sheet on Memory Safety](#)
- [NSA's ESF Securing the Software Supply Chain: Best Practices for Suppliers](#)

FBI

- [Understanding and Responding to the SolarWinds Supply Chain Attack: The Federal Perspective](#)
- [The Cyber Threat - Response and Reporting](#)
- [FBI's Cyber Strategy](#)

National Institute of Standards and Technology (NIST)

- [NIST's Digital Identity Guidelines](#)

- [NIST's Cyber Security Framework](#)
- [NIST's Secure Software Development Framework \(SSDF\)](#)

Australian Cyber Security Centre (ACSC)

- [ACSC's IoT Code of Practice Guidance for Manufacturers](#)

The United Kingdom's National Cyber Security Centre (UK)

- [The UK's Cyber Assessment Framework](#)
- [The UK NCSC's Secure Development and Deployment guidance](#)
- [The UK NCSC's Vulnerability Management guidance](#)
- [The UK NCSC's Vulnerability Disclosure Toolkit](#)
- [University of Cambridge's CHERI](#)
- [So long and thanks for all the bits - NCSC.GOV.UK](#)

Canadian Centre for Cyber Security (CCS)

- [CCCS's Guidance on Protecting Against Software Supply Chain Attacks](#)
- [Cyber supply chain: An approach to assessing risks](#)
- [Canadian Centre for Cyber Security's CONTI ransomware guidance](#)

Germany's Federal Office for Information Security (BSI)

- [The BSI Grundschrift compendium \(module CON.8\)](#)
- [The international standard IEC 62443, part 4-1](#)
- [State of IT-security in Germany report, 2022](#)
- [BSI practices of web application security](#)

Netherlands' National Cyber Security Centre

- [NCSC-NL's Mature Authentication Factsheet](#)

Ma isi

- [How Complex Systems Fail](#)
- [The New Look in complex system failure](#)