TA23-0xxx LAYOUT SBD Shifting The Balance.idml CAUTION: Do not change segment ID or source text V10.1.13 MQ911311 b8d2bd68-593a-482c-b052-731ac63906b3			
ID	**English**	**Kiribati**	**Comment**
1	EMBARGOED DRAFT:	KAKATAI AE BAE NTE TUA:	
2	NOT FOR DISTRIBUTION	TIAKI IBUKIN TE TIBWATIBWAKI	
3	CISA | NSA | FBI | ACSC | CCCS | CERT NZ | NCSC-NZ | NCSC-UK | BSI | NCSC-NL	CISA | NSA | FBI | ACSC | CCCS | CERT NZ | NCSC-NZ | NCSC-UK | BSI | NCSC-NL	
4	NCSC-NO | NÚKIB | INCD | KISA | NISC-JP | JPCERT/CC | CSA | CSIRTAmericas	NCSC-NO | NÚKIB | INCD | KISA | NISC-JP | JPCERT/CC | CSA | CSIRTAmericas	
5	**TLP:CLEAR**	**TLP:CLEAR**	
6	**TLP:CLEAR**	**TLP:CLEAR**	
7	[1]	[1]	
8	**TLP:CLEAR**	**TLP:CLEAR**	
9	SECURE BY{MQ}DESIGN OF CYBERSECURITY	KAMANO MAN{MQ}KARAOANA	
10	SHIFTING THE BALANCE OFCYBERSECURITY RISK:	BITAKIN KANGANGA N TE INTANETE	
11	PRINCIPLES AND APPROACHES FOR	KAINIBAIRE AO ARON KARAOAN	
12	SECURE BY DESIGN SOFTWARE	BWAIN NANON KOMBIUTA AIKA MANO MAN KARAOAIA	
13	**TLP:CLEAR**	**TLP:CLEAR**	
14	**TLP:CLEAR**	**TLP:CLEAR**	
15	**TLP:CLEAR**	**TLP:CLEAR**	
16	**Contents**	**Kanoana**	
17	Overview:	Tarakina:	
18	Vulnerable By Design[1]4	Kairootaki Man Karaoakina[1]4	
19	[1]Whats New[1]6	[1]Bwaai Aika Boou[1]6	
20	How To Use This Document[1]7	Aron Kabonganan Te Beeba Aei[1]7	
21	Secure by Design[1]8	Kamano man Karaoana[1]8	
22	Secure by Default[1]9	Kamano man Teina[1]9	
23	Recommendations for Software Manufacturers[1]9	Taeka ni Bau nakoia Taan Karaoi bwain Nanon Kombiuta[1]9	
24	Software Product Security Principles[1]10	Kainibaire Ibukin Kamonaoan Bwain Nanon Kombiuta[1]10	
25	[1]Principle 1:	[1]Kainibaire 1:	
26	Take Ownership of Customer Security Outcomes[1]11	Kona Bukintaeka n Aron Manoia am Katitamwa[1]11	
27	*[1][2}Explanation*{3][1]11	*[1][2}Kabwarabwarana*{3][1]11	
28	*[1][2}Demonstrating This Principle*{3][1]14	*[1][2}Reiakinaia te Kora ni kaeti aei*{3][1]14	
29	[1]Principle 2:	[1]Kainibaire 2:	
30	Embrace Radical Transparency and Accountability[1]20	Butimwaean Mwakuri aika Kiraati ao aron Bukinam[1]20	
31	*[1][2}Explanation*{3][1]20	*[1][2} Kabwarabwarana* {3][1]20	
32	*[1][2}Demonstrating This Principle*{3][1]21	*[1][2}Reiakinaia te Kora ni kaeti aei*{3][1]21	
33	[1]Principle 3:	[1] Kainibaire 3:	
34	Lead from the Top[1]26	Kairiri mai eta[1]26	
35	*[1][2}Explanation*{3][1]26	*[1][2} Kabwarabwarana* {3][1]26	

36	*[1][2}Demonstrating This Principle*{3][1]27	*[1][2}Reiakinaia te Kora ni kaeti aei*{3][1]27	
37	Secure by Design Tactics[1]28	Kawai n Kamano man Karaoana[1]28	
38	Secure by Default Tactics[1]30	Kawai ni kamano man Teina[1]30	
39	Hardening vs Loosening Guides[1]32	Kamatoatoan vs Kamarauan Kaetieti[1]32	
40	Recommendations for Customers[1]33	Taeka ni Bwai ibukia Katitamwati[1]33	
41	Disclaimer[1][1]34	Te Nangoa[1][1]34	
42	[1]Resources[1]35	[1]Ritioti[1]35	
43	[1]References[1]36	[1]Reburenti[1]36	
44	**OVERVIEW:**	**TARAKINA:**	
45	**VULNERABLE BY DESIGN**	**KAIROOTAKI MAN KAROANA**	
46	Technology is integrated into nearly every facet of daily life, as internet-facing systems increasingly connect us to critical systems that directly impact our economic prosperity, livelihoods, and even health, ranging from personal identity management to medical care.	Rabakau aika boou a riki bwa raora ni waaki ni katoa bong, ngkai bwain-te intanete a katomaira ma bwai aika kakawaki aika kona n roota aron kaubwaira, maiura, ao marurungira naba, ni moa man babarongaan aron kinakim ao aron karaoan mwakuri ni kuakua.	
47	One example of the disadvantage of such conveniences are the global cyber breaches resulting in hospitals canceling surgeries and diverting patient care.	Teuana te kabotau iaon buakakan te waaki aei bon karaoan mwakuri n aonikai nte intanete are a kona ni taoni mwakuri ni korokoro nte Onaoraki ke ni bita aron tararuaia aoraki. n onaoraki	
48	Insecure technology and vulnerabilities in critical systems may invite malicious cyber intrusions, leading to potential safety[1}1{2] risks.	Rabakau aika boon man aki mano n tititem aika kakawaki a kona ni karekei karaoan mwakuri n aonikai nte intanete, ao ni kariki[1}1{2] kanganga. boou	
49	As a result, it is crucial for software manufacturers to make secure by design and secure by default the focal points of product design and development processes.	Ibukin anne, ao e kakawaki irouia taan karaoi bwain nanon kombiuta bwa ana moanibwai kakawakin karaoan bwaai aika mano man karaoaia ao man teia.	
50	Some vendors have made great strides driving the industry forward in software assurance, while others continue to lag behind.	Tabeman taan karaobwai a tia n rangi ni karaoa ae raoiroi n aia karaobwai ni katamaroa te kamano nte intanete, ma tabeman n bon tio naba I buki.	i
51	The authoring organizations strongly encourage every technology manufacturer to build their products based on reducing the burden of cybersecurity on customers, including preventing them from having to constantly perform monitoring, routine updates, and damage control on their systems to mitigate cyber intrusions.	Rabwata ibukin anganakin kariaia a kaungaia taan karaoi rabakau aika boou bwa ana boboto aia karaobwai iaon kauarerekean kanganga nakoia katitamwa ngkana a kabongana te intanete, n aron kabouana, ao tianakin aron te urubwai nakon aia karaobwai ngkana iai mwakuri n tokobito nakon te tititem.	
52	We also urge the software manufacturers to build their products in a way that facilitates automation of configuration, monitoring, and routine updates.	Ti kaungaia naba taan karao bwain nanon kombiuta aika a kona ni karaoi aia mwakuri, n tuoia i bon irouna, ao ni kakaboua kanoana i bon irouna.	
53	Manufacturers are encouraged to take ownership of improving the security outcomes of their customers.	A kaungaki taan karaobwai bwa ana taui aron nako aia waaki ni katamaroa te kamano nakoia aia katitamwa.	
54	Historically, software manufacturers have relied on fixing vulnerabilities found after the customers have deployed the products, requiring the customers to apply those patches at their own expense.	Ngkekei, ao taan karao bwai a karaoi uruaki ma raran n aia bwai imwin kaboakinakona, te mwaan aio are ea karaoia katitamwa bwa ana manga bonota te tititem ni bon oin aia mwane.	
55	Only by incorporating secure by design practices will we break the vicious cycle of constantly creating and applying fixes.	Bon ti man karinan kainibaire ibukin kamano man karaoana ae kona n toki okiokin kanganga ae kakaraoan ao bobonotan te tititem.	
56	**[1}Note:**{2]	**[1}Taeka ni Kauring:**{2]	
57	The term "secure by design" encompasses both secure by design and	Te kibuntaeka ae "mano man karaoana" e ikoti kibuntaeka aika mano man	

	secure by default.	karaoana ao mano man teina.	
58	To accomplish this high standard of software security, the authoring organizations encourage manufacturers to prioritize the integration of product security as a critical prerequisite to features and speed to market.	Ibukin karaoan nanon kainibaire aikai, ao taan anga te kariaia a kaungaia taan karaobwai bwa ana moanibwai karinan kainibaire aikai bwa ana kakawaki riki nakon aron tein aia titem ao mountain kaboakinakona.	deleted
59	Over time, engineering teams will be able to establish a new steady-state rhythm where security is truly designed-in and takes less effort to maintain.	Bon inanon taina, ao intitinia ana kona ni karioi aron mwakuriana aika-teimatoa nte aro are te kamano ea riki bwa aron-teina ao man bebete aron tararuakina.	
60	Reflecting this perspective, the European Union reinforces the importance of product security in the [1}[2}Cyber Resilience Act{3]{4], emphasizing that manufacturers should security throughout a product's life-cycle in order to prevent manufacturers from introducing vulnerable products into the market.	Ni kamanenan te iango aio, aban Eurobe ea kamatoa aron bonganan manon karaobwai nte [1}[2}Cyber Resilience Act{3]{4], ni katerea bwa taan karaobwai a riai ni kateimatoa aia tararua nakon aia bwai n tain-kabonganana nte aro are ana aki kona bwaai aika kai rotaki nte mwakete.	
61	To create a future where technology and associated products are safer for customers, the authoring organizations urge manufacturers to revamp their design and development programs to only permit the shipping of products secure by design and default.	Ibukin taai aika ana roko ike rabakau aika bou ma bwaina nako ana bane ni mano ibukia katitamwa, ao botaki ake anganga te kariaia, a tia ni imanonoia taan karao bwai bwa ana katamaroai riki aia anga ni karaoi ao n ang ate kariaia ibukin kaboan bwaai aika mano man karaoaia ao teina.	boou anga te
62	Well before development, products that are secure by design are conceptualized with the security of customers as a core business goal, not just a technical feature.	Imwain barongaan karaobwai, ao bwaai ake a mano man karaoaia a katameiaki ma te boto ni iango ae manoia katitamwati, tiaki ti aron mwakurina ae kakawaki.	
63	Secure by design products start with that goal before development starts.	Bwaai aika mano man karaoaia a waaki moa ma te kouru imwain moanakin babaronga.	
64	Existing products can evolve to a secure by design state over multiple iterations.	Bwaai aika iai ngkai rabwataia a kona ni mano man karaoaia man karaoan bitaki aika mwaiti.	
65	Secure by default products are those that are secure to use "out of the box" with little to no configuration changes necessary, and security features available without additional cost.	Bwaai aika mano man teia ngaia bwaai ake a kona ni kabonganaki "man bwaokiia" ao ni uarereke aron karaoana, ao mwakuri ni kamano a riai n tauraoi n akea booia.	
66	Together, these two philosophies move much of the burden of staying secure to manufacturers and reduce the chances that customers will fall victim to security incidents resulting from misconfigurations, insufficiently fast customer patching, or many other common issues.	Ikotakin, iango n aika uoua aikai ao ena tar ani kauarerekea te rawawata n aron kamanoaia taan karaobwai ma katitamwa man kanganga ake a rereke man buren kanoan bwaai, ke aki taun ke waeremwen tian bono raran, ao bon kanganga nakon tareboon aika okioki.	tara ni delete
67	The Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), Federal Bureau of Investigation (FBI) and the following international partners[1}2**{2][3}** {2] provide the recommendations in this guide as a roadmap for software manufacturers to ensure security of their products:	Te Kamano nte Intanete ao Botaki ibukin Kamanoan Kateitei (CISA), Botaki ibukin Kamanoan te Aba (NSA), Ana Botaki ni Kakae Rongorongo Tautaeka (FBI), ao raoia tabeman [1}2**{2][3}** {2] a kataurаoi taian taeka ni bau nte booki aei bwa kawai ibukia taan karaobwai ibukin karaoan aia bwaai bwa ana mano.	
68	Australian Cyber Security Centre (ACSC)	Botaki ni Kamano Iaon Intanete mai Aotiteria (ACSC)	
69	Canadian Centre for Cyber Security (CCCS)	Botaki ni Kamano Iaon Intanete ibukin Kanata (CCCS)	
70	United Kingdom's National Cyber Security Centre (NCSC-UK)	Botaki ni Kamano Iaon Intanete mai Buritan (NCSC-UK)	
71	Germany's Federal Office for Information Security (BSI)	Ana Botaki Tautaeka n Tiaman ibukin Kamanoan Rongorongo (BSI)	
72	Netherlands' National Cyber Security Centre (NCSC-NL)	Botaki ni Kamano Iaon Intanete mai Netherlands (NCSC-NL)	
73	Norway's National Cyber Security Center (NCSC-NO)	Botaki ni Kamano Iaon Intanete mai Norway (NCSC-NO)	
74	Computer Emergency Response Team New Zealand (CERT NZ) and New	Ana Tiim Aotearoa ibukin Kanganga nte Kombiuta (CERT-NZ) ao ana	

	Zealand's National Cyber Security Centre (NCSC-NZ)	Botaki ni Kamano iaon Intanete Aotearoa (NCSC-NZ)	
75	Korea Internet & Security Agency (KISA)	Ana Intanete Korea & Botaki ni Kamano (KISA)	
76	Israel's National Cyber Directorate (INCD)	Ana Baba n Tararua Iteraera nte Intanete (INCD)	
77	Japan's National Center of Incident Readiness and Strategy for Cybersecurity (NISC) and Japan Computer Emergency Response Team Coordination Center (JPCERT/CC)	Ana Botaki Tiaban ibukin te Tatauraoi mani Kanganga ao Anga ni Kamano nte Intanete (NISC) ao Ana Tiim Tiaban ibukin Kanganga nte Kombiuta n Tabo ni Babaronga (JPCERT/CC)	add
78	OAS/CICTE Network of Government Cyber Incident Response Teams (CSIRT) Americas	OAS/CICTE Tiim ni Itoman ibukin Kamano iaon Intanete irouia Tautaeka iaon (CSIRT) Amerika	
79	Cyber Security Agency of Singapore (CSA)	Botaki ni Kamano nte Intanete mai Singapore (CSA)	
80	Czech Republic's National Cyber and Information Security Agency (NÚKIB)	Ana Botaki Tautaeka n Czech ibukin Kamano te Intanete ao Kamanoan Rongorongo (NUKIB)	
81	The authoring organizations recognize the contributions by many private sector partners in advancing security by design and security by default.	Botaki ake anganga kariaia a kinai aia katamaroa aia kambwana aomata n aron katamaroan ao karikirakean te kamano man karaoana ao kamano man teina.	
82	This product is intended to progress an international conversation about key priorities, investments, and decisions necessary to achieve a future where technology is safe, secure, and resilient by design and default.	Te boki aei e katauaki bwa ena kaunga te maroro irouia aomata nako ibukin, aanga aika kakawaki, kabwakamwane, ao iango ake e kona iai n reke rabakau aika boou aika mano, a raraoi, ao ni matoa man karaoakina ao teina.	
83	To that end, the authoring organizations seek feedback on this product from interested parties and intend to convene a series of listening sessions to further refine, specify, and advance our guidance to achieve our shared goals.	Ngaia are, taan anga kariaia a kainanoa ami taeka ni buobuoki iaon te boki aei mairouia ake a nano iai ao ake a kan buobuoki n ongongora ara waaki, kamatata, ao ni katamaroa riki ara boki aei e aonga n reke ara kouru ake iroura.	teke
84	For more information on the importance of product safety, see CISA's article, [1}[2}The Cost of Unsafe Technology and What We Can Do About It.{3][4}	Ibukin riki rongorongo iaon bonganan kamanoan bwaai, noora ana boki CISA, [1}[2}Boon kabonganan Rabakau aika boou ao Tera ao ti kona ni karaoia.{3][4}	ae
85	{1}{2]	{1}{2]	
86	1[1} [2]The authoring organizations recognize that the term "safety" has multiple meanings depending on the context its used.	1[1} [2]Taan anga kariaia ataia ae te kibuntaeka ae "kamano" a rawata nanona n aron kabonganana.	
87	For the purposes of this guide, "safety" will refer to raising technology security standards to protect customers from malicious cyber activity.{1]	Ibukin kabonganana nte boki aei, "kamano" e nanonaki iai are kakerakean waaki ni kamano ibukia katitamwa man mwakuri n tokobeto.{1]	
88	**TLP:CLEAR**	**TLP:CLEAR**	
89	2[1} [2]Hereafter referred to as the "authoring organizations."{3]	2[1} [2]Imwiin aei ao ana aranaki bwa "taan anga kariaia."{3]	
90	**TLP:CLEAR**	**TLP:CLEAR**	
91	WHAT'S NEW[1]	BWAAI AIKA BOOU[1]	
92	The initial publication of this report generated a significant amount of conversation within the software industry.	Ngke e moan boretiaki te ribooti aei ao e korakora te maningongo irouia taan karao bwain nanon kombiuta.	
93	Daily news of organizations and individuals being compromised highlights the need for more conversation regarding how to address chronic and systemic problems in software products.	E katoa bong rongorongoia botaki ao aomata ake a rotaki man waki n tokobito aio are ea katurua iai kainanoan riki te maroro iaon kanganga aika a maan man okioki nib wain nanon kombiuta.	aikai ni bwain
94	After the release in April 2023, the authoring organizations (henceforth referred to as "we" and "our") received thoughtful feedback from hundreds of individuals, companies, and trade associations.	Imwin kaotinakoana n Eberi 2023, taan anga kariaia (imwiin aei ao ana aranaki bwa "ngaira" ao "ara") a roko irouia ibuobuoki aika a borongaaki mairouia aomata, kambwana, ao boboti ni iokinibwai.	

95	The most common request in the feedback was to provide more detail on the three principles as they apply to both software manufacturers and their customers.	Te bubuti ae rang okioki bon kainanoan riki kabwaranakoan taian kainibaire ake teniua ao aron rekerekeia ma taan karaobwai ao katitamwa.	
96	In this document, we expand on the original report and touch on other themes such as manufacturer and customer size, customer maturity, and the scope of the principles.	Nte boki aei, ao tina karababa riki ara moan ribooti ao n ringi itera n aron korakoran te tia karaobwai ao katitamwa, ana atatai te katitamwa, ao ai rababan ma rekereken kainibaire.	
97	Software is everywhere and no single report will be able to adequately cover the entire range of software systems, development of software products, customer deployment and maintenance, and integration with other systems.	A roti tabo nako bwain nanon kombiuta ao akea te riboti ae kona ni kabwaranakoi bwain komiuta, aron karaoan bwain nanon kombiuta, aroaroia katitamwa, ao ai aron tomaan bwain nanon kombiuta ma bwaai ake tabeua.	
98	For guidance below that does not clearly map to a particular environment, we look forward to hearing from the community how the practices described in this paper led to particular security improvements.	Ibukin kairi i nano ake aki matata aron kabonganaia n anga tabeua, ti kukurei n ongora mai iroumi anga ake a kona ni kabonganaki ibukin katamaroan waaki ake ti kabwabwarai ikai.	
99	This report applies to manufacturers of artificial intelligence (AI) software systems and models as well.	Te riboti aio e irekereke ma taan karaoi bwain nanon kombiuta aika kona ni iango (AI) ao tein karaoaia naba.	
100	While they might differ from traditional forms of software, fundamental security practices still apply to AI systems and models.	E ngae ngke a kaokoro ma bwain nanon kombiuta ni kawai, ma aron kamano aika kakawaki a irekereke naba ma AI tititem ao tein karaoaia.	
101	Some secure by design practices may need modification to account for AI-specific considerations, but the three overarching secure by design principles apply to all AI systems.	Tabeua aron kamano man karaoaia a kona ni kainnanoa bitakiia ibukin tabeua karaoan-AI, ma ni kabane kainibaire ibukin kamano man karaoana ake teniua ana kairekerekeaki taian AI-tititem.	remove
102	We recognize that transforming a software development lifecycle (SDLC) to align with these secure by design principles is not a simple task and may take time.	Ti kinaa ae aron bitakin karaoan bwain nanon kombiuta (SDLC) ni kainetaki ma kainibaire ibukin kamano man karaoaia aki bebete ao e kona n taua te tai	
103	Further, smaller software manufacturers may struggle to implement many of these suggestions.	Irarikin anne, ao tan karaoi bwain nanon kombiuta ake a uarereke a kona ni iai aia kanganga man irakin kainibaire aikai.	
104	We believe that the software industry needs to make widely available the tools and procedures that make products safer.	Ti kakoaua ae taan karaoi bwain nanon kombiuta a riai n tibwai anga ma aron karaoan bwai aika mano.	
105	As more people and organizations focus their attention on software security improvements, we believe there is room for innovations that will narrow the gap between larger and smaller software manufacturers to the benefit of all customers.	Ngkai ea tiraua riki aomata ao botaki aika a kabotoa aia mwakuri iaon katamaroan kamano, ao ti kakoaua ae ena reke angan katamaroa ake ana kona ni kauarerekea te maranga imarenaia taan karaobwai ake a bubura ao uarereke ao man mabiao katitamwati iai.	
106	This update to the original secure by design report is part of our commitment to build partnerships with the many interconnected stakeholder communities that underpin our technological ecosystem.	Te kaboou aei nakon te riboti are mai mwaina iaon kamano man karaoakia e irekereke ma nanora ni kan karaoi irekerekera ao ara itoman ma rabwata ao boboti ake ngaia aan ara rabakau aika boou.	
107	It is the result of feedback from many parts of that ecosystem, and we will continue to listen and learn from perspectives.	Bon man mwiin aia taeka ni boutoka man mwangan nako ara rabakau aika boou, ao tina teimatoa n ongora ao n reirei man aia iango nako.	
108	Although there are many challenges ahead, we are incredibly optimistic as we learn more about people and organizations that have already adopted a secure by design philosophy, often with success.	E nage ngke e tiraua kanganga aika ti kona ni kaitarai, ma ti ti rangi n onimaki ngkai ti kona n reirei aroia aomata ao rabwata ake a tia n kabongana aron kamano man karaoana, ao angiin te tai e nakoraoi.	
109	**TLP:CLEAR**	**TLP:CLEAR**	
110	**HOW TO USE THIS DOCUMENT**	**ARON KABONGANAN TE BOKI AEI**	
111	[1]We urge software manufacturers to adhere to the principles within this	[1]Ti kaumakiia taan karaoi bwain nanon kombiuta bwa ana iri raoi	

	document.	kainibaire nte boki aei.	
112	Software manufacturers can demonstrate their commitment by publicly documenting their actions taken, in line with the steps listed below.	A kona taan karaoi bwain nanon kombiuta ni kaota nanoia man katanoataan bwai ake a karaoi, ake a irekerereke ma kawai aika i nano.	
113	We encourage software manufacturers to find tactics that meet the spirit of this principle and to create artifacts that will build a compelling case to even skeptical current and potential customers that they are embodying the secure by design philosophy.	Ti kaungaia taan karaoi bwain nanon kombiuta bwa ana karioi aia anga ake ana irii nanon kainibaire ao man karaoi bwaai ake ana kona n anai nanoia katitamwa aika ngkai ao n taai aika ana roko ae a iri nanon kainibaire ibukin te kamano man karaoana.	iri
114	In addition to actions software manufacturers should take, customers can also leverage this document.	I rarikin aia kawai aikai ao taan karaoi bwain nanon kombiuta ana ataia, ae katitabwa a kona ni iriri kanoan te boki aei.	m
115	Companies buying software should ask hard questions of their vendors, drawing inspiration from the examples of adhering to the principles listed in this document.	Kambwana ake a kakaboi bwain nanon kombiuta a riai n titiraki mwaaka nakoia taan kabonakoi bwaai, ao man karioi aia titiraki man irakin kainibaire aika nte boki aei.	
116	In doing so, customers can help to shift the market towards products that are more secure by design.	Karaoan aio, ao katitamwa a kona ni ibuobuoki ni ibita te mwakete ni biiti karaobwai nakon ake a mano man karaoaia.	
117	An example of questions customers can ask of vendors is given in [1}[2}CISA's Guidance for K-12 Technology Acquisitions.	Katoto n titiraki ae a kona ni kabongana katitamwa nakoia taan karaobwai a reke nte [1}[2}CISA Kairi ibukin Anakin te Rabakau ae boou ae K-12.	
118	{1]{2]We encourage enterprise customers to incorporate these practices into procurement processes, vendor due diligence assessments, enterprise risk acceptance decisions, and other steps taken when evaluating vendors.	{1]{2]Ti kaungaia kambwana ake a bobobwai bwa ana kabonganai anga aikai inanon aia waakin aia bobobwai, ukerana raoi bwa a koaua, atakin kanganga, ao anga riki ake a kakaraoaki nakoia taan kabonakobwai.	delete
119	Customers should also push their vendors to publicly document the secure by design actions each vendor takes.	Katitamwati a riai nab ani kairoroia taan mwakete bwa ana kaoti anga ake a kabonganai ibukin te kamano man karaoana.	naba ni
120	Collectively, this can create a strong demand signal for security, which can encourage and enable software manufacturers to take steps towards greater security.	Bonnanoana, ao e kona ni karika kainanoan te kamano ae korakora, aei e kona ni kaungaia ao ni angania taan karaobwai te kan karaoi kawai ibukin te kamano ae tamaroa riki.	n
121	In other words, just as we seek to create a pervasive secure by design philosophy within software manufacturers, we need to create a "secure by demand" culture with their customers.	Nanona naba ngkanne, bwa ngkai ti imanonoa aron ukoran te rabakau ni kamano man karaoana irouia taan karaobwai, ti kainanoa naba te "kamano man kainanoana" irouia aia katitamwa.	
122	**Secure by Design**	**Kamano man Karaoana**	
123	"Secure by design" means that technology products are built in a way that reasonably protects against malicious cyber actors successfully gaining access to devices, data, and connected infrastructure.	"Kamano man karoana" e nanonaki iai are rabakau aika boou ana riai ni karaoaki n angaia are ana mano iai katitamwa man waaki n tokobito aika naoraoi iaon te intanete, rongorongo, ao kateitei ake a toma.	nakoraoi
124	Software manufacturers should perform a risk assessment to identify and enumerate prevalent cyber threats to critical systems, and then include protections in product blueprints that account for the evolving cyber threat landscape.	Taan karaoi bwain nanon kombiuta a riai ni karaoi tuoan ao warebwaian kanganga ake a okioki man te intanete ibukin totokoaia, ao ana manga karini aron kamano ake a tia ni koreaki ibukin kanganga nte intanete ake a bibitaki aroia.	
125	Secure information technology (IT) development practices and multiple layers of defense— known as defense-in-depth—are also recommended to prevent malicious actors from compromising systems or obtaining unauthorized access to sensitive data.	Aron karaoan kamano ibukin rabakau ibukin rongorongo (IT) ao totoko aika uatao— a ataaki n araia ae totoko-ae-nano—a katauaki naba kabonganakiia ibukin totokoan mwakuri buaka ake a kona n rotii tititem ke n reke iai angan anakin rongorongo aika kakawaki.	
126	The authoring organizations further recommend manufacturers use a tailored threat model during the product development stage to address all potential threats to a system and account for each system's deployment	Taan anga kariaia a kaungaa taan karaobwai ana kabongana te anga n totoko ae barongaki n tain uaboboan karaobwai aonga ni kona n kaitarai kanganga nakon aia tititem ao n atai naba aron tein ma mwakurin aia	kaungaia

	process.	tititem.	
127	The authoring organizations urge manufacturers to take a holistic security approach for their products and platforms.	Taan anga kariaia a kairoro bwa taan karaobwai ana kabongana aron kamano aika bwanin aroia ibukin aia bwai nako.	
128	Secure by design development requires the strategic investment of dedicated resources by software manufacturers at each layer of the product design and development process that cannot be "bolted on" later.	Karaoan kamano man karaoaia e kainnanoa te karinmwane ae barongaaki nakoia taan karaobwai n tain nako karaoana ao aron nako karaoana ae na aki kona n tangira "kamatoana" rimwi.	
129	It requires strong leadership by the manufacturer's top business executives to make security a business priority, not just a technical feature.	E kainnanoa te kairiri ao matoa mairouia taan kairiri nte bitiniti ni karaobwai ibukin karaoan kamano bwa ana moanibwai, ao tiaki ti ibukin aron karaoana.	
130	This collaboration between business leaders and technical teams extends from the preliminary stages of design and development, through customer deployment and maintenance.	Te reitaki i marenaia taan kairiri ao taan mwakurii karao bwaai e moa man moan babarongan karaoana, ni karokoa ae roko irouia katitamwa ao ai karaoan mwakurian katamaroa.	karaobwai
131	Manufacturers are encouraged to make hard tradeoffs and investments, including those that will be "invisible" to the customers (e.g., migrating to programming languages that eliminate widespread vulnerabilities).	A kaungaaki taan karaobwai bwa ana karaoi karinmwane ao waaki ni karaobwai aika matoa aroia ni ikotaki ma ake "aki nooraki" irouia katitamwa (e.g., bitakin kabonganan taetaen kombiuta ake aki kai rotaki).	missing word nakon
132	They should prioritize the features, mechanisms, and karementation of tools that protect customers rather than product features that seem appealing but enlarge the attack surface.	A riai ni moanibwaia karaoana, ao teina, ao ni karaoi anga ake ana kamanoia katitamwa nakon are ana moanibwaia karaona ake ana nang anainano ma e rereke iai aron tokobito.	
133	There is no single solution to end the persistent threat of malicious cyber actors exploiting technology vulnerabilities, and products that are "secure by design" will continue to suffer vulnerabilities; however, a large set of vulnerabilities are due to a relatively small subset of root causes.	Akea te anga n takarere ae ena kona n totokoi nako aia anga n tokobito kamwarua n kumei memeren rabakau aika boou, ao bwai ake a "mano man karaoakia" ana bon rorotaki; ma, angin memere a rereke man kanganga aika a okioki naba.	
134	Manufacturers should develop written roadmaps to align their existing product portfolios with more secure by design practices, ensuring to only deviate in exceptional situations.	Tan karaobwai ana riai ni karaoi ao ni koroi kawai ake ibukin tein aia bwai bwa ana airiri ma kainibaire ibukin kamano man karaoaia, ao ni kona ni katibanakoia man kainibaire ngkana ea bon riai.	CHECKED
135	The authoring organizations acknowledge that taking ownership of the security outcomes for customers and ensuring this level of customer security may increase development costs.	Taan anga kariaia a ataia ae katauan bukinaki ibukin aia kamano nakoia katitamwa ao kakoauana bwa e koro nanon waaki ni kamano nakoia katitamwa e kona ni karaka boon karaoakia.	
136	However, investing in secure by design practices while developing innovative technology products and maintaining existing ones can substantially improve the security posture of customers and reduce the likelihood of compromise.	Ngaia are, karaoan te kamano man karaoana iaon kukune aika boou ake a kateimatoai kamanomano nakon mwaneka ake imwina ibukia katitamwa a kinaki bwa ana bwai te tia karaobwai.	
137	Secure by design principles not only strengthen the security posture for customers and brand reputation for developers but the practice also lowers maintenance and patching costs for manufacturers in the long term.	Kainibaire ibukin kamano man karaoana aki tii kakorakorai taian kamano nakoia katitamwa ma e na kabura aran te kambwana are e karaoi ao ni kauarerekei taian mwakuri n tararua ao itera ni kabanemwane irouia taan karaobwai inanon te tai ae maan.	
138	The Recommendations for Software Manufacturers section listed below provides a list of product development practices and policies for manufacturers to consider.	Aika inano bon taian Taeka ni bau, ibukin aron karaoan bwai ao kainibaire ibukia taan karaobwai bwa ana noori man karioi aia iango mai iai.	i nano
139	CISA | NSA | FBI | ACSC | CCCS | CERT NZ | NCSC-NZ | NCSC-UK | BSI | NCSC-NL	CISA | NSA | FBI | ACSC | CCCS | CERT NZ | NCSC-NZ | NCSC-UK | BSI | NCSC-NL	
140	NCSC-NO | NÚKIB | INCD | KISA | NISC-JP | JPCERT/CC | CSA |	NCSC-NO | NÚKIB | INCD | KISA | NISC-JP | JPCERT/CC | CSA |	

	CSIRTAmericas	CSIRTAmericas	
141	**TLP:CLEAR**	**TLP:CLEAR**	
142	**TLP:CLEAR**	**TLP:CLEAR**	
143	[1]	[1]	
144	**Secure by Default**	**Kamano man Teina**	
145	"Secure by default" means products are resilient against prevalent exploitation techniques out of the box without added charge.	"Kamano man Teina" nanona bwa karaobwai a taubobonga ni kaitarai kanganga ake ana kona ni kaoti n aki manga tangira te kabanemwane.	
146	These products protect against the most prevalent threats and vulnerabilities without end-users having to take additional steps to secure them.	Taian karaobwai aika a kona ni kaitarai kanganga n aekaia nako n akea kainanoan te tia kamanena ni karaoi taian kawai ni kamanomano irarikina.	
147	Secure by default products are designed to make customers acutely aware that when they deviate from safe defaults, they are increasing the likelihood of compromise unless they implement additional compensatory controls.	Kamano man teina bon karaobwai ake a bon tia aroia ibukia katitamwa ni kona n ataia bwa enga ae mano ibukia n teina**,**n te karaobwai ake ana kona ni karika te kamangaongao ni karokoa are a kamaeu mwin riki taian totoko ibukin kaitaran kamangao akanne.	add comma
148	Secure by default is a form of secure by design.	Kamano man teina e mena i aan ana karinan kamano man karaoana.	
149	A secure configuration should be the default baseline.	Te kamano are e a tia ni karaoaki bon anne ae boboto iai tein te karaobwai anne.	
150	Secure by default products automatically enable the most important security controls needed to protect enterprises from malicious cyber actors, as well as supply the ability to use and further configure security controls at no additional cost.	Kamano man teina bon aron te karaobwai are e a bon kaman maeu te kamanomano ae rangi ni kakawaki ibukia taian bitineti ibukin totokoaia taan aonikai, n raonaki ma te kona ni kamanenai riki kamanomano ake iaona riki n aron manga kamaeuan riki tabeua n akea te kabanemwane	i aona
151	The complexity of security configuration should not be a customer problem.	Aron kamaeuan riki taian kamanomano aikai e naaki riki bwa ana kanganga te katitamwa.	
152	Organizational IT staff are frequently overloaded with security and operational responsibilities, thus resulting in limited time to understand and implement the security implications and mitigations required for a robust cybersecurity posture.	Taan mwakuri n te kombiuta~~T~~n taabo nako a bon rangi n tabetabe ibukin tararuan ao kabutan te tabo ni mwakuri, are ea kona ni kauarerekea aia tai ni karaoi mwakuri ni kamanomano ni kaitarai mwakuri n aonikai.	add
153	Manufacturers can aid their customers by optimizing secure product configuration—securing the "default path"—ensuring their products are manufactured, distributed, and used securely in accordance with "secure by default" standards.	Taan karaobwai a kona ni katuraoi ao kabebetei aron kamanenaan ao kammwakuran—kamano "n aron teina"—ao ni ibuobuoki nakoia katitamwati ni kataubobongai raoi, n tibwatibwaki, angania te kona ni kabonganai iaan te "kamano man teina" ae bwainaki n te aonnaba.	
154	Manufacturers of products that are "secure by default" do not charge extra for implementing added security configurations.	Karaobwai n "kamano man teina" akea te tiati iai ibukin kamaeuan riki taian kamanomano ake iaona riki.	
155	Instead, they include them in the base product like seatbelts are included in all new cars.	Ma enga n anne, ngkai a kaman tia ni karinaki inanon te karaobwai kanga ai aekakin te kabaebae ni kaintekatekan te kaa ae boou.	
156	***Security should not be a luxury option, but should be considered a right customers receive without negotiating or paying more.***	***Te kamano tiaki te karaka aro, ao a riai n taraki katitamwa bwa ana reke irouia n akea te boraraoi ke te manga bwakamwane.***	

157	RECOMMENDATIONS FOR SOFTWARE MANUFACTURERS	KATAMAROA NAKOIA TAAN KARAOBWAI	
158	This joint guide provides recommendations to manufacturers for developing a written roadmap to implement and ensure IT security.	Taian kaeti aikai ana anga taian katamaroa nakoia taan karaobwai ibukin kabobongan te boki ibukin te kawai ae e na iraki are e na karaoaki bwa ena kateimatoi kamanoaia IT.	
159	The authoring organizations recommend software manufacturers implement the strategies outlined in the sections below to take ownership of the security outcomes of their customers through secure by design and default principles.	Te rabwata ibukin boretiakin taian rongorongo n te intanete e katauiia taan karao bwain nanon kombiuta ni waki nakon kainibaire ake a kaotaki n te mwakoro ae inano bwa ngaai ae ana bon oioi mai irouia te kamanomano ibukia aia katitamwa rinanon te kainibaire are te kamano man karaoana ao kamano man teina.	ngaia
160	**TLP:CLEAR**	**TLP:CLEAR**	
161	**SOFTWARE PRODUCT SECURITY PRINCIPLES**	***KAINIBAIRE IBUKIN TE KAMANO MAN KARAOBWAI***	
162	Software manufacturers are encouraged to adopt a strategic focus that prioritizes software security.	Taan karaoi bwain nanon kombiuta a kaungaaki bwa ana kabonganai anga ake ana moanibwai manon aia karaobwai.	
163	The authoring organizations developed the following three core principles to guide software manufacturers in building software security into their design processes prior to development, configuration, and shipment of their products.	Te rabwata ibukin boretiakin taian rongorongo n te intanete a karaoi teniua kainibaire ibukin kairaia taan karao bwain nanon kombiuta ibukin te kamanomano inanon tain karaoakin bwain nanon kombiuta, te katamaroa, ao ai kanakoan aia karaobwai.	
164	[1]	[1]	
165	**Take ownership of customer security outcomes[1}** {2][3}and evolve products accordingly.	**Ana buki taan karaobwai ni kamanoaia katitamwa [1}** {2][3}ao man bibiti karaobwai ibukin kamano.	
166	The burden of security should not fall solely on the customer.{1]	Ena aki riki te kamanomano bwa ana kanganga te katitamwa.{1]	
167	**Embrace radical transparency and accountability.**	**Kabuta nakoa taekana bwa ena kiraati.**	
168	Software manufacturers should pride themselves in delivering safe and secure products, as well as differentiating themselves from the rest of the manufacturer community based on their ability to do so.	Taan karao bwain nanon te kombiuta ana riai n ata kakawakin te karaobwai ae mano ao n akea ana kanganga, ao ni iai okorona ma taan karaobwai ae tabeman.	
169	This may include sharing information they learn from their customer deployments, such as the uptake of strong authentication mechanisms by default.	Aio e rekereke ma tibwaan rongorongo ake a bwaati imwin kaotinakoan aia karaobwai nakoia katitamwa, n aron kabonganan angan aron kinakim man tein te karaobwai.	
170	It also includes a strong commitment to ensure vulnerability advisories and associated common vulnerability and exposure (CVE) records are complete and accurate.	N raonaki ma kabanean aron aia karaobwai n aron bonotan raran ke memere ni bwain nanon te kombiuta (CVE) ae tabwanin man eti.	
171	However, beware of the temptation to count CVEs as a negative metric, since such numbers are also a sign of a healthy code analysis and testing community.	E ngae n anne, tarai ngkami man taian anainano ni kabarekareka ake ana warekaki bwa kabuakakan te CVEs, bwa man te ware aikai ao e na kaotara raoi marurungin mwin mwakurian ao mwin tuoana irouia aomata.	
172	**Build organizational structure and leadership to achieve these goals.**	**Katean rabwata aika barongaaki ao te waki ni kairiri ibukin uarokoan kouru aikai.**	
173	While technical subject matter expertise is critical to product security, senior executives are the primary decision makers for implementing	Ngkai oin waki a boboto man aia itera taan rabakau ake a mwatai iaon kakawakin te kamanomano n te karaobwai, taan kairiri ake mai ieta bon	

	change in an organization.	ngaia taan karaoi babaire ibukin karaoan bitaki.	
174	Executives need to prioritize security as a critical element of product development across the organization, and in partnership with customers.	A riai taan kairiri ni kabanei aia tai ni moanibwaia kakawakin te kamanomano man bwain kombiuta, ao ni ikarekebai ma katitamwati bwa a riai ni matata n te karaobwai anne:	▪
175	**1**	**1**	
176	**2**	**2**	
177	**3**	**3**	
178	CISA | NSA | FBI | ACSC | CCCS | CERT NZ | NCSC-NZ | NCSC-UK | BSI | NCSC-NL	CISA | NSA | FBI | ACSC | CCCS | CERT NZ | NCSC-NZ | NCSC-UK | BSI | NCSC-NL	
179	NCSC-NO | NÚKIB | INCD | KISA | NISC-JP | JPCERT/CC | CSA | CSIRTAmericas	NCSC-NO | NÚKIB | INCD | KISA | NISC-JP | JPCERT/CC | CSA | CSIRTAmericas	
180	**TLP:CLEAR**	**TLP:CLEAR**	
181	**TLP:CLEAR**	**TLP:CLEAR**	
182	[1]	[1]	
183	To enable these three principles, manufacturers should consider several operational tactics to evolve their development processes.	Man kainibaire aika teniua ao, taan karaobwai a riai ni karaoi aia kawai ae ana uaana inanon tain te karaobwai.	i nanon
184	Convene routine meetings with company executive leadership to drive the importance of secure by design and secure by default within the organization.	Ana tewea te maroro ma taan kairiri n te kambwana bwa ena buti n aki tokitoki karaoan te kamano man karaoana ao teina inanon aia rabwata nako.	
185	Policies and procedures should be established to reward production teams that develop products adhering to these principles, which could include awards for implementing outstanding software security practices or incentives for job ladders and promotion criteria.	Kainibaire ma aro ni kairiri ana kaungai karekean kaniwanga nakoia kain te tiim ni karaobwai ake a iri nanon kainibaire, n reitaki ma kaniwanga ibukin karaoan te kamanomano ae rakai riki baana ni bwain nanon te kombiuta ao ni boutoka te wakirake ao anainano.	
186	Operate around the importance of software security to business success.	Waaki aika a kakawaki ibukin kamanoan bwain nanon kombiuta ibukin bitineti bwa ana bura ieta.	
187	For example, consider assigning a "software security leader" or a "software security team" that upholds business and IT practices that directly link software security standards and manufacturer accountability.	Te katoto, karekean temanna bwa e na riki bwa te "mataniwi ibukin kamano man bwain nanon kombiuta" ibukin bitineti ao ibukin mwakurin taian kombiuta ni uarokoi nakon kamanomano aika bwainaki n te aonnaba ao taan karaobwai bwa ana okiraki ni mwiin aia mwakuri.	
188	Manufacturers should ensure they have robust, independent product security assessment and evaluation programs for their products.	Ana kakoauaa taan karaobwai bwa e tamaroa kamanoan aia karaobwai, ni kanganga rinnakoana ao ni karaoi kawai ibukin tuoan aia karaobwai.	
189	Use a tailored threat model during resource allocation and development to prioritize the most critical and high-impact features.	Ana kabonganai anga n totoko aika barongaaki n tain mwanenakina ao karaoana ao ni moanibwaia arona aika kakawaki man korakora-riki.	
190	Threat models consider a product's specific use-case and enables development teams to fortify products.	Anga n totoko ana riai n tara teuana aron-kabonganana ao n anganiia aia intinia bwa ana otangai karaobwai.	
191	Finally, senior leadership should hold teams accountable for delivering secure products as a key element of product excellence and quality.	Ao te kabanea, taan kairiri ake ieta a riai ni karaoa te rekenikai nakoia intinia ake a karaoi bwai bwa aio boton uaiakinan te tamaroa ao te nakoraoi.	
192	As part of the October 2023 update to this guidance, these three	Teuana mai buakon taian kaboou n Okitobwa 2023, ao kainibaire aikai a	

	principles are expanded upon through the following explanations, demonstrations, and evidence.	karababaki riki n aron kabwarabwara, kaotioti, ao kakoaua aikai.	
193	**PRINCIPLE 1:**	**KAINIBAIRE 1:**	
194	[1}Take Ownership of Customer Security Outcomes{2]	[1}Kona Bukintaeka ngkana aki Mano am Katitamwa{2]	
195	**EXPLANATION**	**KABWARABWARA**	
196	[1}Modern best practices dictate that software manufacturers invest in product security efforts that include **{2][3}application hardening, application features,**{2][5} {2][7}and application **{2][9}default settings.** {2]	[1}Kawai n taai aikai a taku bwa taan karaobwai ana kabanei kaubwaia ibukin karaoan kamano nakon aia bwai n aron **{2][3}kamatoan karaoabwai, aron kabonganan karaobwai,**{2][5} {2][7}ao aron **{2][9}barongakin teina.** {2]	
197	[1}Software manufacturers need to implement **{2][3}application hardening**{2][1} by using processes and technologies that raise the cost for a malicious actor wishing to compromise applications.	[1}Taan karaobwai a riai ni kateimatoai **{2][3}kamatoan aia karaobwai**{2][1} mani kabonganan anga ae ena rangi ni bobuaka aron kumetoan karaobwai irouia.	
198	Application hardening protocols and procedures help products resist attacks by intelligent malicious actors.	Aron mwakurian ao kainibaire ibukin kamatoan karaobwai a kona ni ibuobuoki n totokoi tokobito mairouia taan iowawa aika niniwana.	
199	Terms like hardening, product security, and resilience are all closely related to product quality.	Kibuntaeka n aron kamatoa, manon karaobwai, ao aki ururuakiia a nang irekereke ma nakoraoin karaobwai.	
200	The idea is that security must be "baked in," and not "bolted on." \[1] By baking in security, software manufacturers can not only increase their customers' security but also increase their products' quality.	Te kantaninga bwa te kamano e riai n "rin inanona," ma ena aki "toka iaona." \[1] Man rinna inanona, ao taan karaobwai aki ti kona ni karakai kamano nakoia katitamwa ma a karakai naba nakoraoin aia karaobwai.	
201	Sample tactics include ensuring user input is validated and sanitized, and isn't entered directly into code (i.e., by using parameterized queries instead), using a memory safe programming language, rigorous software development life cycle (SDLC) management, and using hardware-backed cryptographic key management.	Aikai anga tabeua n aron ukeran koaua bwa te tia kabongana te karaobwai ana eti ao ni itiaki, ao man aki rin nte burokuraem. (i.e., man kabonganan titiraki aika kakaokoro), kabonganan te burokuraem ae mano ana ururing, barongan kawaekoan karaoan karaobwai (SDLC), ao ai kabonganan reitaki nte koroboki aika iai-nneia.	
202	Applications need to support **{1][2}application features**{1][4} that relate to cybersecurity.	A kainanoaki karaobwai aika boutoka **{1][2}tein karaobwai**{1][4} aika rekereke ma te kamano nte intanete.	
203	Sometimes called "capabilities," these features extend the functionality of a product or service in ways that help maintain or increase the security posture of a customer.	Tabetai aranaki bwa "konabwai," tein karaobwai aikai a kabwaka maiun ao mwakurin karaobwai aikai nte aro bwa ana mano iai katitamwa.	
204	Sample security-related features include supporting transport layer security (TLS) for all network connections, single sign on (SSO) support, multi-factor authentication (MFA) support, security event audit logging, role-based access control (RBAC), and attribute-based access control (ABAC).	Aikai anga tabeua aika rekereke ma aron-kamano boutokan kamano aika uatao n tain butin(TLS) te intanete, boutokan ae ti teuana angan(SSO)rinim, boutokan aron kikina-ae mwaiti(MFA), karekean tain otetanakin karaobwai, aron te Karin man-nakoam(RBAC),aron te Karin man-kinakim (ABAC).	butin (TLS) angan (SSO) rinim nakoam (RBAC), aron
205	Some of these product features are configurable allowing customers to more easily integrate the product into their existing environments and workflows.	Tabeua tein karaobwai aikai a kona ni bitaki nakon are a tangiria katitamwa nte aro bwa ana kona ni karokoa nakon aia otabwanin ma butin aia mwakuri.	
206	Those configurations mean applications must have **{1][2}default settings**{1][4} set until customers configure them.	Tein karaobwai akanne ana ira nanon **{1][2}barongakin teina**{1][4} ni karokoa ae a bitia katitamwa.	
207	Those default settings need to be set securely "out of the box" so that customers expend fewer resources to make their stack of technology products more secure.	Aron barongakin teina e kainanoa ae ena man "ao man aki numwaroaki" aonga katitamwa ni uarereke aia kabanemwane ibukin karaoan aia karaobwai ae mano.	

208	Each of these elements – application hardening, application security features, and application default settings – plays a role in the security of the application, and the resulting security posture of the customer.	Bwai aikai ni kabane – kamatoan karaobwai, ana anga ni kamano te karaobwai, ao barongakin tein karaobwai – a rangi ni kakawaki ibukin manon te karaobwai, ai aron tein kamanoan te katitamwa.	
209	Software manufacturers should think about each of these elements and how they relate to each other.	Taan karaobwain nanon kombiuta a riai ni iangoi raoi bwai aikai ao ni angoi aroi bwa ana kanga ni kabonganai n tain aia karaobwai.	iangoi
210	Manufacturers should think about more than just their investments to incorporate these elements into their products.	Taan karaobwai a riai ni iangoi tiaki ti aron aia karekemwane ngkana a karini anga ni katamaroa aikai.	
211	Manufacturers should take it a step further and consider how those elements change the real-world security posture of their customers, for better or for worse.	Taan karaobwai a riai n tara riki are iaona ao n taraia bwa ana kanga anga ni katamaroa aikai ni bita aron kamano nte-aonnaba ao aia katitamwa, ena katamaroa ke ena kabuakaka.	ibukin ae tamaroa ke ae buakaka
212	Manufacturers should take ownership of their customers' security outcomes rather than measuring themselves solely on their efforts and investments.	Taan karaobwai ana riai ni bukintaeka n aron kamanoaia aia katitamwa ao ana aki tii tara aia mwakuri bwa tao a mwakuri korakora ke ea korakora te kabanemwane.	
213	The responsibility should be placed upstream, with the manufacturers, where it has the greatest likelihood of reducing the chances of compromise.	Te kabukintaeka a riai n turuturu iai naake ieta, ao kambwana ni karaobwai, karaoan aio ena kaurerekea reken te kanganga ni mwakuri n tokobito.	add
214	Unfortunately, that's not the case today.	Te kabuanibwai, bwa tiaki anne teina ae nonoraki ni bong aikai.	
215	Too many manufacturers place the burden of security on the customer rather than investing in comprehensive **{1][2}application hardening.**	Ea nang tiraua taan karaobwai ae a katuka te bukinaki irouia katitamwa ao man rawa ni kabanemwane iaon **{1][2}kamatoan karaobwai.**	
216	{1][2}For example, when the manufacturer patches one vulnerability, we often see similar vulnerabilities exposed because they addressed the symptom rather than the root cause of that defect.	{1][2}Te katoto, ngkana te tia karaobwai e bonota teuana te memere, ao tiaki toki n noria bwa bwai ni bonobono aika a manga raran iaan are a karaoa kanokinaean te kanganga ao aki kumea botona.	aikai i
217	The product might implement different mitigations in various parts of the code base for the same class of vulnerability.	Te karaobwai e kona ni karioi aron totoko aika okoro nte burokuraem ibukin karinan memere aika titabo teia.	
218	As a case in point, after the manufacturer fixed one input sanitization vulnerability, researchers or attackers found code paths that did not benefit from the improved input sanitization.	Te kabotau ae tamaroa, ao imwin karaoakin te raran teuana man kanakoan taeka aika karika te kanganga nte burokuraem, ao taan ukeuke ma taan tokobito ana kunei taekan burokuraem aika aki kona ni mabiao mai iai bwa are ea tia ni katamaroaki taekan te burokuraem.	
219	The manufacturer applied fixes one at a time rather than unifying the codebase to eliminate that class of vulnerability across the entire application.{1]	Taan karaobwai a kakaraoi raran teuana imwin teuana, ngke ana riai ni kanakoi taekan burokuram ake a kakarika tokobitoan te karaobwai.{1]	remove
220	**[1}Application features**{2][3} can create both benefits and risk for customers.	**[1}Aron kunimwanian karaobwai**{2][3} e kona ni karika te kukurei ke te maraia nakoia katitamwa.	mabiao
221	Features that allow integration points with many external systems and versions can greatly increase the value of a product.	Karaoan karaobwai aika kona n toma ma karaobwai riki tabeua ma teia nako e kona n karakaa boon te karaobwai.	
222	And yet supporting features without a retirement plan, like a networking protocol, can leave customers vulnerable if they lack an understanding of the implications of ongoing use of that feature.	Ma aron karaoan karaobwai ake akea tokin taia, n aron te katomatoma, ena katikuia katitamwa bwa ana kai rotaki ngkana a kabi ni kabongana tein karaobwai aika aki totoki.	
223	For example, some products continue to use networking protocols that have their origins in the 1990s or 2000s and are now known to be unsafe.	N aron te kabotau, tabeua karaobwai a kabongana te katomatoma aika karaoaki n 1900 ko 2000 tabun ake a ataki bwa aikoa mano.	
224	There are numerous factors that can slow how fast customers upgrade and deploy modern security measures.	E tiraua bukin ae kona ni karaurau aron baitin kerakem nte karaobwai ao kaotinakoan anga ni kamano aika boou.	

225	They may use products that integrate with the rest of the organization's network, but lack modern security measures, preventing the IT team from modernizing.	E kona n ae a kakabonganai katomatoma man ana tabo te tia karaobwai, n akean kamano aika boou, aio e totokoa aia mwakuri ni ka boou IT.	
226	Still, software manufacturers can factor these patterns into their planning process to encourage customers to stay current.{1]	Ma a boni kona naba, taan karaobwai ni Karin kanganga aikai n tain aia babaronga a aonga ni unga katitamwa ni kakaboui aia tititem{1]	k
227	**[1}Application default settings**{2][3} are an added area of potential risk for customers.	**[1}Barongakin tein karaobwai**{2][3} a kona ni karekei riki kanganga nakoia katitamwa.	
228	Manufacturers often choose certain default settings, making it easier for customers to use the application features they want.	Aki naba toki taan karaobwai n rinei tabeua tein barongan karaobwai, ae ena kabebetea riki aron kabonganan aia karaobwai irouia katitamwa.	
229	The downside is that this practice increases the attack surface for customers who may not need certain features and protocols that are enabled by default.	Buakakan karaoan aio bwa e kona riki ni karababai anga ke aroaro n tokobitoa te karaobwai are e maiu man tein karaoana.	
230	Additionally, many security controls are toggled off by default or require customers to take time to configure their settings to increase security.	Ni ikotaki ma anne, ao angiin anga n totoko a kanakoaki n tain karaoaia nte aro are katitamwa manga bon tabeia karaoan tein karaobwai ibukin kamanoaia.	
231	Explicit threat modeling is a tactic that may help inform the decision of which features should be on by default or which settings are needed to be secure by default.	Karaoan raoi katotongan kanganga bon te anga teuana ae kona ni ibuobuoki ni kaoti iango ake a kona iai ni karaoaki iai aron tein taian kamano man tein karaobwai.	add
232	Another tactic is to investigate ways to make features more discoverable for the administrator.	Teanga naba teuana bon kakaean anga ake ana karaoi tein karaobwai bwa ana bebete rekeia irouia taan kamwakuria.	Te anga
233	Some manufacturers ship products with defaults that can create risk for some or all their customers.	Tabeman taan karaobwai a kabonakoi karaobwai aika a kona iai n reke kanganga nakoia aia katitamwa.	
234	Rather than set safer defaults, they often opt to produce a **{1][2}hardening guide**{1][4} that customers must implement at their own expense.	Aki karaoi tein aia karaobwai, a karaoi **{1][2}kaetieti ni kamatoa**{1][4} are ana manga karaoi katitamwa ni bon oin aia kabanemwane.	
235	Hardening guides suffer from several common problems.	A tiraua kanganga aika rereke man kaetieti aika matoa.	
236	Some hardening guides are hard to find and are not well supported.	Tabeua kaetieti aika matoa a kanganga warekaia ao aki rangi ni boutokaki.	
237	Others are complex to implement, occasionally requiring software development to write an extension module.	Tabeua a kanganga iran nanoia, ao angina te tai e kainnanoa karaoan boki ni kaetieti aika abwawaki.	remove abwabwaki
238	Still, others assume the reader has extensive cybersecurity experience to understand the ways in which various settings change the attack surface.	Ao tabeman, a kataua naba bwa te tia wareware e korakora ana atatai iaon te kamano nte intanete ao ni kona ni karaoi tein aia karaobwai bwa ana mano.	
239	Practitioners who have an incomplete understanding of the ways in which attackers work may fail to properly implement hardening guide instructions, especially if the instructions do not make the trade offs clear.	Taan kabonganai karaobwai ake aki bwanin aia atatai n aron aia kumeto kamwarua a kona ni kabi raoi aron irakin kaetieti ni kamatoa, riki ngkana e aki raoi rangi n ota irouia buakakan karaoan kaetieti ni kamatoa.	
240	Further, not all hardening guides are written by engineers who are intimately familiar with attacker tactics and economics, causing them to create hardening guides that are ineffective even if faithfully implemented.	N reitia ma anne, ao ti tabeua kaetieti ake a bon koreaki irouia intinia aika mwatai n aron anga n tokobito ao aron boona, aei are akona iai ni karaoi kaetieti ni kamatoa aika aki bongana engae ngke a iri raoi nanoia.	a kona e ngae
241	Millions of customers are taking on the responsibility to harden multiple instances of software or systems, often in resource-constrained environments.	Mirion katitamwati a karaoi nanon kaetieti ni kamatoa ma uarereken aia atatai ibukin karaobwai ao tititem, riki n tabo ake a karako kaubwaia.	

242	Relying on hardening guides simply doesn't scale.	Onimakanan kaetieti ibukin kamano ni kamatoa e aki kona n raka arona.	
243	An application's settings should be continuously evaluated whether the settings were the default or set by the customer, against the manufacturer's current understanding of the threat landscape.	Katamaroan te karaobwai e riai n ririnanoaki engae ngke e riki man teina ke a karaoia katitamwa, karaoan aio e riai ni irira aron keraken aia konabwai taan karaobwai.	
244	Applications should be made with clear indicators about the potential risks that may result from those settings and should make those indicators known.	Karaobwai a riai n ati iaoia kanganga ake akona n reke ngkana e bitaki aron kamanoana man teina a riai ni kaotii raoi.	i aoia
245	Just like a modern car has an indicator about seatbelts and expresses that indicator by sounding an alert if you try to drive without buckling up, software should express indicators about the state of security of a system.	N ai aron te ka ae iai aron kaotan kanganga ngkana e aki bae te roo ao ena riai naba n tangtang ni kaotia ae aki bae room, karaobwai ana riai naba ni kaota korakoran te kamano man aia tititem.	
246	If an application is configured to not require MFA for administrator accounts, it should make the administrators regularly aware that they and their entire organization are in danger if they do not configure MFA.	Ngkana te karaobwai e karaoaki bwa ena mwakuri n akean te MFA irouia taan kamwakuria, e riai ni iai te kakauring nakon te tia kamwakuri karaobwai ae te kambwana ae tabwanin aki mano nte karaobwai ao a riai ni karaoa te MFA.	
247	Additionally, if an application is configured to support older protocols that are now known to implement weak cryptography, it should regularly make it clear to the administrators that the organization is in danger and provide resources to resolve the situation.	Ni ikotaki ma anne. ngkana te karaobwai e boutokai kawai ngkoa are a ataaki bwa e kobonganai ang ani karaba aika memere, e riai ni kakauringiia taan karaobwai n atongnga bwa aia boboti e na reke nte kanganga ao n ana riai ni katauraoi ritioti ibukin katokan aia kanganga.	comma
248	We urge manufacturers to implement routine nudges that are built into the product rather than relying on administrators to have the time, expertise, and awareness to interpret hardening guides.	Ti kaungaia taan karaobwai bwa ana kakaraoi kaunga nano aika a nim ma aia tein aia karaobwai nakon are a nang katabeia taan kabongana bwa ana iai aia tai, rabakauia, ao atakin aron kabwaranakoan kaetieti ni kamatoa.	
249	Opportunities clearly exist for innovation to balance security and usability considerations.	E ataki ae iai ang ni katamaroa ibukin kabaretan aron te kamanomano ao kabonganan karaobwai.	anga
250	Each of the above elements creates an untenable situation in which customers need to research, fund, purchase, staff, deploy, and monitor additional **{1][2}security products**{1][4} to reduce the chance of compromise.	Nikabane bwai ake a taekinaki i eta a karika te aro ae riai ni karaoaki irouia katitamwa bwa ana riai ni ukeuke, mwanena, kaboa, kateirakeia taan mwakuri, kaotinakoi, ao taratarai riki **{1][2}karaobwai ni kamanoe**{1][4} ni kauarerekea te ananga n tokobitoaki.	
251	Small and medium sized organizations (SMOs) are generally unable to facilitate these options.	Boboti aika uarereke ao aika tau buuraia (SMO)n teina ao ena kuri ni kanganga karaoan aio.	(SMO) n
252	They face scarcity in expertise, funding, and time which taxes bandwidth and function, forcing security to a lower priority, and, in the aggregate, exacerbates collective risk.	Aia kanganga bon akeaia ke karakon tan rabakau, mwane, ao te tai n taekiti aia intanete ao ni waaki, are ea karika te kamano bwa tiaki te moanibwai, ao, n bon tokina, reken kanganga aika mwaiti.	
253	Conversely, security investments by the relative few manufacturers will scale.	N teina, ao katamaroan te kamano man oin aia kabanemwane tabeman tan karaobwai ena bubura mwiina.	
254	A common phrase that summarizes the problem is that the software industry needs more secure products, not more security products.	Te kibu n taeka ae uarereke ibukin te kanganga aei e kangai bwa taan kabonganai bwain nanon kombiuta a kainnanoi riki karaobwai aika mano, nakon karaobwai ni kamano.	
255	Software manufacturers should lead that transformation.{1]	Taan karao bwain nanon kombiuta a riai ni kaira te bitaki aio.{1]	
256	**TLP:CLEAR**	**TLP:CLEAR**	
257	***The software industry needs more secure products, not more security products.***	***Taan kabonganai bwain nanon kombiuta a kainnanoi riki karaobwai aika mano, nakon karaobwai ni kamano.***	

258	***Software manufacturers should lead that transformation.***	***Taan karao bwain nanon kombiuta a riai ni kaira te bitaki aio.***	
259	Today, we sometimes read comments from manufacturers explaining that a customer was compromised due to not enabling a particular security feature or following specific hardening guidance.	N tai aikai, ao ti kona ni wareki aia rongorongo ni kabwarabwara taan karaobwai ae te katitamwa e tokobitoaki ibukina bwa e aki kamaua aron te kamano teuana ke e aki iri nanon tabeua kairi ibukin kamatoan kamano.	
260	Instead, after a compromise, manufacturers should explain whether a particular security feature or specific hardening guidance would have prevented the compromise and consider making it the default at no charge.	Ni bon etina, ao imwin te tokobito, ao taan karaobwai a riai ni kabwarabwara bwa ena riki aio ngke arona bwa a kamauaki kamano ni kamatoa ke aron kamano ao ana riai ni karaoi bwa kamano n tein aia karaobwai n akea boona.	
261	In those cases where the product itself was not sufficiently hardened in the design and implementation phases, the manufacturer should explain how they are working to eliminate that class of vulnerability from their product lines.	Ngkana e riki aio bukina bwa aki tau kamatoa n aron karaoana n tain katameiana ao mwakuriana, ao te tia karaobwai e riai ni kabwarabwara aroia ni mwakuria kamaunanakoan utun waaki n toobito akanne.	tokobito
262	Software manufacturers have a responsibility to ensure that their products are designed and developed with security as a top priority.	Taan karaoi nanon kombiuta iai tabeia bwa ana karaoa aia karaobwai mani barongaia raoi ni moanibwaia aron te kamano.	
263	To that end, they should **[1}objectively measure the results**{2] of their efforts in the field.	N tokina, ao ana riai n **[1}warebwaia raoi mwiin ana urubwai**{2] ma korakoraia nte itera anne.	
264	We call on manufacturers to not just focus on their internal efforts, but to objectively measure and regularly report the results and effectiveness of a product's security efforts and configurations, and to build a feedback loop that creates changes in the SDLC that lead to measurable improvements in customer safety and more secure products.	Ti katanoata ikai nakoia taan karaobwai bwa ana tarai raoi korakoraia, ma ana warebwai raoi mwin ana urubwai ao ni kakatanoata mwiin ma nakoraoin korakoraia ni karao kamano ma anga, ao ni karaoa te anga n riboti rikaki ae ena kairia nakon katamaroa aika kona n tauaki mwiia ibukin katamaroan te kamano ao karaon bwai riki aika mano.	nakoraoi n
265	Reporting should include anonymized data that the academic and security research community could use to track high-level trends and measure progress ecosystem wide.	Aron riboti a riai ni kairi rongorongo aika raba are ana kona iai bwakuaku ao taan ukeri aron kamano aika raka-aroia ao ni kona ni warebwaiaki aroia irouia nako taan kabongana.	
266	**DEMONSTRATING THIS PRINCIPLE**	**REIAKINAN TE KORA NI KAETI AEI**	
267	Software manufacturers and online services should find ways to demonstrate successes in implementing this principle.	Taan karaobwai ao taan ibuobuoki nte intanete a riai ni kunei kawai ni kawarabwarai tokanikai ake a reke man karaoan te kainibaire aei.	
268	They should seek to provide evidence in the form of artifacts for outsiders to examine.	A riai ni tauraoi ni katauraoi bwai ni kakoaua ibukia ake tiaki kain aia kamironron bwa ana tuoi.	n
269	No single artifact by itself will prove that a manufacturer is implementing a robust secure by design program, but by providing various artifacts they will build a case of the manufacturer's commitment to developing secure products.	E aki kona teuana te bwai ni kakoaua ni kaotia ae te tia karaobwai ea tia ni katauraoi burokuraem ibukin anga ni kamano man karaoana, ma man katauraoan bwai ni kakoaua aika mwaiti ao a kona ngkanne ni kakoauaki ae te tia karaobwai e nanona aron karaoan karaobwai aika mano.	
270	This approach is in the spirit of "show, rather than tell."	Te kawai aei e karaoaki man te taeka are"karaoia, ma tai tataekinna."	
271	To demonstrate this principle, software manufacturers should consider steps such as those in the following list.	Aron kabwaranakoan te kora ni kaeti aei, ao taan karaobwai a riai ni iangoi aikai.	
272	The authoring organizations recognize that few software manufacturers will be able to immediately implement these practices and produce corresponding artifacts at the start of their secure by design journey.	Taan anga te kariaia a kiina ae tabeua taan karaoi kanoan kombiuta a kona ni karaoi kawai aikai nte tai ae waekoa ao ni katauraoi bwai ni kakoaua nte tai are iai karaoan kamano man karaoana.	
273	Further, software manufacturers will need to prioritize this list depending on how the customers deploy the product in the field to achieve the	I rarikin anne, ao taan karaoi bwain kombiuta a kainanoa ae ana moanibwaii aikai nakon aroia katitamwa bwa ana kanga ni kaotinakoi	

	largest security benefits.	karaobwai ni karekei kabwaia aika bubura man kamanomano.	
274	**SECURE BY DEFAULT PRACTICES**	**ANGA NI KAMANO MAN TEINA**	
275	**Eliminate default passwords.**	**Kanakoi taeka ni kamano ake a kaman rin.**	
276	[1}Default passwords continue to be implicated as the cause of many attacks every year.	[1}Taeka ni kamano ake a kaman rin a bon tabe naba ni kakariki anga n tokobito ni katoa ririki.	
277	Making a commitment to eliminate this chronic problem will deny easy access to attackers.	Karaoan tauannano ibukin kamaunan te kanganga aei ena kona n tuki riniia taan tokobito.	
278	Similarly, manufacturers should consider what password practices should be implemented, such as minimum password length and disallowing known breached passwords. {1]	Ai ti tearona naba, ngkana taan karaobwai a karaoi anga ibukin taeka aika raba, n aron kabwabwakan passwords ao katabuakan kabonganan kibuntaeka aika a tia n tokobitoaki. {1]	te arona
279	**Conduct field tests.**	**Karaoi tutuo.**	
280	[1}As technology continues to evolve and become more complex, it is increasingly important for software manufacturers to conduct security-centric user testing to understand their products' security posture in the field.	[1}Ngkai ea rikirake rabakau aika boou man bibitaki ao ni kanganga aroia, ea rikirake naba kakawakin karaokin tuoan-manon karaobwai bwa aonga n atai aron manenan ao kabonganan karaobwai ni kamano.	
281	Similar to how user research informs software development requirements, software manufacturers should also conduct security-focused user research to understand where the security user experience (UX) falls short.	Ai ti te arona naba ma ukeraia katitamwa ae kobonganaki ibukin barongan karaoan karikirake, taan karaobwai a riai naba ni karaoi tuoan-kamano mai irouia katitamwa aonga n atai nanoia aomata (UX) aia karaobwai.	a n add
282	By observing how customers deploy and use their products in real-world environments, software manufacturers can gain valuable insights into the usability and effectiveness of their security features and controls.	Man tarataran aroia katitamwa ngkana a kabonganai aia karaobwai, ao taan karaobwai a kona n reke irouia kantaninga ma aron taratara aron kabonganan ao raoiroin aia kawai ni kamano.	
283	These insights can help identify areas for improvement and refine their products to better meet the security needs of customers.	Taratara aikai a kona ni ibuobuoki ni kakaean anga ni katamaroa ao ni manga katamaroa riki aia karaobwai ni kaitarai kanganga ni kamano.	
284	For example, field tests might suggest changes in UX flow, defaults, alerting, and monitoring.	Te kabotau, te ukenano n anga iango ibukin bitaki n nanoia aomata, n aron teia, kauring, ao taratarakina.	
285	Field tests may also show where past improvements in the product's design reduce the velocity of security patches, reduce configuration errors, and minimize attack surface. {1]	Ukeraia katitamwa e kona ni kaota aron katamaroan karaobwai ake a kauarerekea birin karaoan bono raran, ake a kauarerekei kairua, ao ake a kauarerekea aron te tokobito. {1]	
286	Manufacturers should consider the following:	A riai n tarai itera aikai taan karaobwai:	
287	Do customers correctly implement the hardening guide?	A eti raoi karaoan kaetieti ni kamatoa irouia katitamwa?	
288	Do the product's existing security features perform as expected in the field?	N aron Tein karaoan kamano a mwakuri nakon are kantaningaki maim win tuoaia?	t
289	Do those features actually resist real-world attacks?	A bon totokoi tokobito taian karaobwai ke aki?	
290	Which features would better reduce the likelihood of compromise?	Enga mai buakon tein te karaobwai ae kauarerekei aron tokobito?	
291	*Note:*	*Taeka ni Kauring:*	
292	*To gain deeper insights into these elements, software manufacturers may wish to partner with customers to conduct red team exercises to see how the product resists attacks.*	*Ibukin kananoan riki taratara iaon anga aikai, ao taan karaoi bwain nanon kombiuta a kona ni iraorao ma katitamwa ni karaoi kakamwakuri irouia kain aia tiim n tutuo aron mwakuri aia karaobwai n totokoi tokobito.*	n add
293	*These field tests might take place at the customer's physical site, virtually, or via telemetry from the application in a privacy-preserving manner.*	*Tabo n tutuo aikai a kona ni karaoaki n aia tabo katitamwa, nte intanete, ke nte eea man te karaobwai n te aro ae kamanoi-rabaia.*	
294	**Reduce hardening guide size.**	**Kauarerekei kairi ibukin kamatoa.**	

295	[1}Manufacturers can improve customers' security postures by streamlining or even eliminating product hardening guides and focusing on the most critical security measures that customers should prioritize when deploying their products.	[1}A kona taan karaobwai ni katamaroa aron kamanoaia katitamwa man kauarerekean ke bon kakean kairi ni kamatoa ao n kaoioi aia mwakuri iaon anga ni kamano ake a riai ni moanbwaii katitamwa ngkana a kabonganai aia karaobwai.	
296	Rather than overwhelming customers with a laundry list of security measures, manufacturers should identify the top security risks that their products are susceptible to and provide clear and concise guidance on how to mitigate these risks.	Man kabebeteaia aia katitamwa ma anga aika mwaiti ibukin kamanoaia, taan karaobwai a riai n rinei kanganga ni kamano ake a moamoa riki man aia karaobwai ao ni katauraoi kairi iaon aron katokan kanganga aikai.	
297	In addition, manufacturers should provide customers with tools and automation that simplify the process of implementing security controls, such as scripts that can easily be deployed in their environment.	Irarikin anne, ao taan karaobwai a riai ni katauraoi bwaai ao automation aika a kona I kabebetea aron karaoan bwai ni kamano, n aiaron taekan te kamano ao na bebete kaotinakoana n aia otabwanin.	kabebete ni ena
298	These tools should additionally be able to verify and clearly show the changes made from the original baseline.	Bwai aikai a riai nab ani kona n tuoi raoi ao ni kamatatai raoi bitaki ake a reke man tein karaoana.	naba ni
299	By streamlining hardening guides and providing customers with easy-to-use tools and automation, manufacturers can reduce the burden on their customers and help ensure that their products are deployed in a secure manner.	Man kauarerekean kairi ni kamatoa ao man anganakia katitamwa bwai ni ibuobuoki aika bebete-aron-kabonganakia ao man mwakuri ibon irouia, taan karaobwai a kona ni kauarerekei rawawata nakoia katitamwa ao ni buobuoki ni kakoauaa ae aia karaobwai a kaotinakoaki nte aro ae mano.	
300	One tactic would be to consider implementing the Pareto principle to reduce the number of steps for the common use cases (the 80%), and then providing contextual guidance and tooling for less common scenarios (the 20%).	Anga teuana bon iangoan kabonganan te Pareto kainibaire are kauarerekea mwaitin kawai ibukin kabonganana ake a okioki (80%), ao katauraoan kairi ake a buoka aron te ota ao aron kabonganan bwai ni ibuobuoki nakon (20%).	
301	In this way, software manufacturers will be making the simple things simple, and the hard things possible.	Nte aro aei, ao tan karaoi bwain nanon kombiuta a karaoi reirei aika bebete bwa ana bebete, ao ake a matoa bwa ana kona ni karaoaki.	
302	Field testing will be a powerful tool in measuring how long it takes customers to discover, understand, and implement hardening guides.	Tutuoana ena riki bwa te bwai ni buobuoki n aron warebwaian mania katitamwa ni kaotaia, n oota, ao ni karaoi kairi ibukin te kamatoa.	
303	Manufacturers should consider how the product could nudge administrators to take action within the product itself rather than relying on them to implement tasks from a hardening guide.{1]	Taan karaobwai a riai ni iangoi aia karaobwai bwa ana kanga ni kaungaia taan kabongana bwa ana mwakuri i bon irouia ao tiaki are ana katang iaoia taan kabongana bwa ana karaoi mwakuri man kaetieti ni kamatoa.{1]	
304	**[1}Actively discourage use of unsafe legacy features.**{2]	**[1}Mwakuria aron aki kaungaan kabonganan tein karaobwai aika a maan ao aki mano.**{2]	
305	[1} Prioritize security through clear upgrade paths over backwards compatibility.	[1} Moanibwaia aron kamano man kakabouana ae itiaki ao tiaki n anga aika a maan.	
306	Publish blog posts showing the adoption of safer features and protocols, and deprecate unsafe features by announcement, possibly from within the product itself.	Boreti rongorongo ni kaota arom ni kabonganai kawai ao anga aika mano, ao taobarai aroaro aika aki mano ni katanoatai, bon inanon te karaobwai.	add
307	A significant number of customers have demonstrated that they will not keep their systems current with modern network, identity, and other critical security features.	A tiraua mwaitia katitamwa aika kaotia bwa a rawa ni katomaia ma tititem aika boou, ao ang ani kamano tabeua aika kakawaki.	anga ni
308	In some cases, customers fear existing functionality will break with an upgrade.	Ao tabemwaang, a maaku mwakurin aia tititem bwa a kona ni uruaki ngkana a kaboui.	maaka
309	By making upgrades as seamless as possible, customers will likely	Man karaoan kakabou aika bebete man kakaireke, ao katitamwa ana unga	

	upgrade and get security fixes more often and quickly.	nanoia ni kakabou ao ni karekei kamano ni bonoraran nte tai ae waekoa.	
310	Software manufacturers should aggressively nudge customers along upgrade paths that reduce customer risk.{1]	Taan karaoi bwain nanon kombiuta a riai ni kaungaia aia katitamwa ibukin kakabou aika ana kauarerekei aia kanganga.{1]	
311	**[1}Implement attention grabbing alerts.**	**[1}Karaoi kauring aika anainano.**	
312	[1]{2][3}Similar to seat belt chimes in cars that continuously make noise when seat belts are not fastened, manufacturers should implement timely and repeated alerts when users or admins are in truly unsafe states, warning administrators that they are using deprecated protocols in their environments and suggest upgrade paths.	[1]{2][3}E titabo ma are kabonganan te roo nte kaa are aki toki ni kakarongoa ngkana e aki bae, taan karaobwai a riai ni karaoi anainano aika tainaki man okioki ngkana taan kabongana a bon aki mano raoi, kauringia taan kabongana ae a kabonganai anga aika taorikakaki n aia otabwanin ao tuangia aroia n kakaboui.	
313	Implement timely and repeated alerting when users or admins, or the application configuration, are in an unsafe state.	Karaoi kauring aika tainaki ao man okioki ngkana taan kabongana, ke tein karaobwai, a bon aki mano.	
314	Make the unsafe mode clear to the administrators on a regular basis.	Kaota aron teaki mano bwa ena matata nakoia taan kabongana ni kakaokiokia.	te aki
315	An additional feature could require a super administrator to acknowledge the lack of MFA on their account upon each login, or even disable certain key features until they enable MFA.	Tein karaobwai aika boou ena kainnanoa te tia kabongana are mai ieta bwa ena kariaia ae ana akaunti e aki MFA ngkana e rinnako, ke kamatei tein karaobwai tabeua ngkana akea ana MFA.	
316	There is room to innovate to achieve these goals while not creating alert fatigue.{1]	Iai anga n karaoi ao ni karekei taian kouru aikai ae ena akea iai te kainnano man okiokin kakauring.{1]	
317	**[1}Create secure configuration templates.**	**[1}Karaoi taiboran aron kaetana aika mano.**	
318	[1]{2][3}These templates can pre-set certain configurations to safe settings based on an organization's risk appetite.	[1]{2][3}Taibora aikai ana kona n kaman-tia iai aron kaetana nakon te settings ae mano ae ni boboto iaon bwaruan te kabuanibwai nakoia kambwana.	
319	While it might be overly simplistic to have low/medium/high security templates, that example illustrates how many settings could be updated to manage risk for the organization.	Tao ena tara n rangi ni mangori taran ae iai iroum taibora aikai, ma te katoto anne e katerei mwaitin tein karaobwai ake a kona ni kabouaki ni babairei kanganga nakon te kambwana. uareke/tau/bubura	missing
320	Templates can be supported by hardening guides on the risks the manufacturer has identified.{1]	Taibora aikai ana boutokaki man kaetieti ibukin kamatoa ibukin kanganga ake ea a tia ni atai te tia karaobwai.{1]	n
321	**TLP:CLEAR**	**TLP:CLEAR**	
322	**TLP:CLEAR**	**TLP:CLEAR**	
323	[1]	[1]	
324	**SECURE PRODUCT DEVELOPMENT PRACTICES**	**KAMANOI ARON KARIOAN KARAOBWAI**	
325	**Document conformance to a secure SDLC framework.**	**Iran nanon Boki ma tein te karaobwai SDLC ae mano.**	
326	[1}Secure SDLC frameworks provide objectives and examples across people, processes, and technologies.	[1}Tein ana karaobwai SDLC ena tauraoi iai kouru ao katoto irouia aomataa, aron karaoaia, ao rabakau aika boou.	delete
327	Consider publishing a detailed description of which secure SDLC framework controls have been implemented and describe any alternate controls which have been used.	Iangoia bwa ena boretiaki kabwarabwara aika matata ni irekereke ma aron tauan mwiin tein ana karaobwai SDLC ae mano ana tia ni karaoaki ao kabwarabwarai ngkana iai aron tauan mwiin bwai ake a tia ni kabonganaki.	
328	Within the US, consider using the NIST Secure Software Development Framework (SSDF).	Nte US, iangoia bwa kona kabongana te NIST Aron Karaoan bwain te Intanete ae Mano (SSDF)	
329	While not a checklist, the SSDF "describes a set of fundamental, sound practices for secure software development."{1]	E ngae ngke tiaki te beba n tututuo, te SDDF "e kabwarabwarai rinanin baika kakawaki ibukin, kawain karioan karaobwai aika mano."{1]	

CHECKED

330	**Document Cybersecurity Performance Goals (CPG) or equivalent conformance.**	**Kouru ibukin Bokin Nakoraoin Mwakurin Kamanomano nte Intanete (CPG) ke katoto riki aikai iri nanona.**	
331	[1}When an organization attests that they conform to the NIST SSDF standard, they are asserting that their SDLC is informed by well-understood best practices.	[1}Ngkana taan karaobwai a taku bwa airi nanon ana kainibaire NIST SSDF, a bon taku naba ngkanne bwa aia SDLC a karaoi ao man ata-raoi tikiraoin kabonganana.	
332	However, it is not sufficient for them to only have a robust SDLC.	Ma, e aki tau bwa ana ti iai irouia te SDLC ae tikiraoi.	
333	They also need to protect their own enterprise and development environments from malicious actors who would seek to manipulate the security properties of the product while it is still in development.	A kainnanoi naba kamanomano ibukin aia kambwana ao aia tabo ni karioi karaobwai bwa ana mano mairouia kamwarua ake a kan tokobitoa aron tein aia karaobwai inanon tain karioana.	
334	This is not a theoretical class of attack, but one that has been carried out with adverse effects to customers, and by extension national security.	E aki taekinaki aron te tokobito aio kanga te kario, ea tia n ririki aio ao katitatamwa a tia n namakini kanganga, ao riki a tian aba n rotaki botaki ni kamano tautaeka.	delete
335	Organizations should consider publishing details on the organization's conformance to the CISA CPGs, the NIST Cybersecurity Framework (CSF), or other cybersecurity program frameworks.{1]	Kambwana a riai ni iangoia bwa ana boreti taekan nako iran nanon CISA CPGs, Aron tein ana kamano nte Intanete NIST (CSF), ao ai anga ni kamano nte intanete riki tabeua.{1]	
336	**[1}Vulnerability management.**{2]	**[1}Babarongan Memere.**{2]	
337	[1} Some manufacturers have a vulnerability management program that focuses on patching vulnerabilities discovered internally or externally, and little more.	[1} Tabeman taan karaobwai iai aia burokuraem ibukin barongan memere ae boboto iaon bonotan memere ake a reke inanon ke tinanikun aia kambwana, ao tabeua riki.	
338	More mature programs incorporate extensive data-driven analysis of vulnerabilities and their root causes, taking steps to systemically eliminate entire classes of vulnerability{1][2}3{1][4}.	Burokuraem ake a mwatai iai inanona aron kabwaranakoan memere ma aron rikia aika rio man-rongorongo, ao anga n karaui ni kamaunanakoi aekan nako katei ni memere{1][2}3{1][4}.	
339	They implement formal programs around setting quality planning, quality control, quality improvement, and quality measurement.	A karaoi burokuraem man kainibaire aikai baronga aika nakoraoi, aron tiatianakin aika nakoraoi, katamaroa aika nakoraoi, ao ai warebwai aika nakoraoi.	a
340	They view defect management as a business matter, not merely a security matter.	Ao a tarai barongan nakobuaka bwa tabeia, ao tiaki ti ibukin te kamano.	
341	These programs are not dissimilar in some ways to quality and safety programs in other industries.{1]	Burokuraem aikai titabo n teina tabeua ma te katamaroa ao te anga ni kamano n bitiniti tabeua.{1]	
342	**[1}Responsibly use open source software.**	**[1}Kabonganai raoi bwain nanon kombiuta ake akea booia.**	
343	[1]{2][3}When open source software is used, be responsible by vetting open source packages, fostering code contributions back to dependencies, and helping sustain the development and maintenance of critical components.	[1]{2][3}Ngkana a kabonganaaki bwain nanon kombiuta ake aki kaboaki, kabonganai raoi man tuoi raoi bwain nanona, ao kaungai karaoan burokuraem nakoia taan kabongana, ao ibuobuoki n aron boutokan barongan ao katamaroan bwaina aika kakawaki.	
344	For reference, Japan's Ministry of Economy, Trade, and Industry (METI) has published {1][2}[3}"Collection of Use Case Examples Regarding Management Methods for Utilizing OSS and Ensuring Its Security."{4]{1]	Ibukin ritioti ao, Ana Tabo ni Mwakuri Tiaban ibukin Kaubwai, Iokinibwai ao Karikirake (METI) ea tia ni boreti {1][2}[3}"Botan nako mwakuri ao katoto ibukin aron Barongan ao Kabonganan OSS ao Kakoauan ana Kamano"{4]{1]	reburenti
345	**[1}Provide secure defaults for developers.**	**[1}Katauraoi kamano man teia ibukia taan kario.**	
346	[1]{2][3}Make the default route during software development the secure one by providing safe building blocks for developers.	[1]{2][3}Karaoi taian kawai man teia n tain karioan bwain nanon kombiuta ae mano man katauraoan buraoki ibukia taan kario.	
347	For example, given the prevalence of SQL injection vulnerabilities causing	Te katoto bwa, ngkai ea rangi n tabangaki memere karinan SQL inanon	

CHECKED

	real-world harm, ensure that developers use a well-maintained library to prevent that class of vulnerability.	raran man karaoi kanganga aika ataki-i aonnaba, koaua raoi bwa tan kario a kabonganai karaoaki-raoi ibukin totokoan katei ni memere akanne.	
348	Also known as "paved roads" or "well-lit paths," this practice ensures both speed and security, and reduces human error.{1]	Ataki naba n araia ae "te kawai ae katamaroaki" ke "kawai aika ota-raoi," te kawai aei e kakoauaki bwa e reke te buti ma kamano, ao kauarerekei karaoan kairua.{1]	
349	**[1}Foster a software developer workforce that understands security.**	**[1}Kaungai karikaia taan mwakuri ni kario aika ata aron te kamano.**	
350	{1][2}Ensure that your software developers understand security by training them on secure coding best practices.	{1][2}Kona riai n ataia raoi bwa taan karioi bwain nanon kombiuta a ota n aron te kamano man reiakinaia iaon aron kabonganan burokuraem aika mano aika tamaroa.	
351	Further, help transform the broader workforce by updating hiring practices to evaluate security knowledge and working with universities, community colleges, bootcamps, and other educators to weave security into computer science and software development curriculums.{1]	Irarikin anne, buobuoki ni ibita ao katirauaia taan mwakuri ni kario man kakabouan aron am kammwakuri n ririnanoi rabakauia iaon te kamano ao reitaki naba ma kuura aika ririeta, reirein te tautaeka, taabo ni kataneiai, ao tanna reirei nte aro are kona kona n rarangai kanoan kamano ibukin kombiuta ma aron karaoan reiakinan karaobwai. {1]	
352	3[1} [2]NIST SSDF, PO 1.2, Example 2:	3[1} [2]NIST SSDF, PO 1.2, Katoto 2:	
353	"Define policies that specify the security requirements for the organization's software, and verify compliance at key points in the SDLC (e.g., classes of software flaws verified by gates, responses to vulnerabilities discovered in released software)."{1]	"Kawenei kainibaire aika ana kamatata aron wakin te kamano nakon ana karaobwai te kambwana, ao tuoa raoi iran nanoia n aron tein te SDLC (e.g., kabwakan karinan raranin karaobwai a tuoaki man te mataroa, totoko nakon raran a kuneaki n karaobwai aika tia n otinako."{1]	
354	**[1}7.[2]{3][4}Test security incident event management (SIEM) and security orchestration, automation, and response (SOAR) integration.**{3]	**[1}7.[2]{3][4}Tuoi aron barongan kanganga nakon te kamano (SIEM) ao aron katoman babairean kamano, mwakuri ibon irouna, ao anga n totoko (SOAR).**{3]	
355	In addition to conducting field tests, work jointly with popular SIEM and SOAR providers in conjunction with select customers to understand how incident response teams use logs to investigate suspected or actual security incidents.	Ni ikotaki ma karaoan tututuo, reitaki ni mwakuri ma taan katauraoi SIEM ao SOAR aika kinaki n ronaki irouia tabeman katitamwa bwa e aonga n ota aron kabonganan bwai ake tauaki mwiia bwa e aonga ni kona ni ukoraki kanganga aika a tia riki ao aika taian kataunaari.	
356	Few software developers have experience responding to an incident and may create log entries that don't help responders as much as they would expect.	Tabeman taan karioi karaobwai a tia n namakina ae totokoan kanganga e kona ni kariki tauan mwiin karinrin ae aki roko arona n aron are a kantaningaia.	
357	By working both with SIEM and SOAR technologies and real incident response professionals, the development team can create logs that tell the correct and complete story, saving time and reducing uncertainty during an incident.	Man te reitaki ni mwakuri ma rabakau aika bou man SIEM ao SOAR ao ma kanganga ake a tia n reke ma taan mwakuri, te tiim ni kario e kona ni karaoi aron taun mwiin rinanako are e kona ni ang ate karaki ae eti ao e tabwanin, e aki kangtai ao man aki karika te nano uoua n tain kanganga.	
358	**[1}8.[2]{3][4}Align with Zero Trust Architecture (ZTA).**	**[1}8.[2]{3][4}Airiri ma Banna ae Akea ae Onimakinaki (ZTA).**	
359	{1]Align product deployment guides with, for example, the NIST ZTA models and the [2}[3}CISA Zero Trust Maturity Model{4]{1].	{1]Ka airiri kairi ibukin kaotinakoan karaobwai ma, kanga te kabotau iai, ana tamei NIST ZTA ao te [2}[3}CISA Akea ae Onimakinaki Tamei aika a Matoa {4]{1].	
360	Encourage customers to incorporate these principles in their environments.	Kaungaia katitamwa bwa ana kamanenai kainibaire aikai n aia otabwanin.	
361	CISA | NSA | FBI | ACSC | CCCS | CERT NZ | NCSC-NZ | NCSC-UK | BSI | NCSC-NL	CISA | NSA | FBI | ACSC | CCCS | CERT NZ | NCSC-NZ | NCSC-UK | BSI | NCSC-NL	

362	NCSC-NO | NÚKIB | INCD | KISA | NISC-JP | JPCERT/CC | CSA | CSIRTAmericas	NCSC-NO | NÚKIB | INCD | KISA | NISC-JP | JPCERT/CC | CSA | CSIRTAmericas	
363	**TLP:CLEAR**	**TLP:CLEAR**	
364	[1]	[1]	
365	**PRO-SECURITY BUSINESS PRACTICES**	**KAWAIA BITINITI AKE A NANONI-KAMANO**	
366	**[1}Provide logging at no additional charge.**	**[1}Katauraoi tauan mwin rinnako n akea booia.**	
367	{1]Cloud services should commit to generating and storing security-related logs at no additional charge.	{1]Taan katauraoi tiewa a riai n kataua bwa ana karaoi ao n kawakini tauani mwin rinnako ake a rekereke ma-kamano n akea te manga kabwakamwane.	
368	On-premises products should likewise generate security-related logs at no additional charge.	Karaobwai ake bwain-auti a riai naba ni karaoi tauani mwin rinnako ake a rekereke ma-kamano n akea te manga kabwakamwane.	
369	Further, the product should log security events by default since many customers may not understand their value until after an incident.	Irarikin anne, man teini karaobwai ao a riai ni kona n taui mwiin bwai ake a riki ngkai angia katitamwa aki atai kakawakia ni ua e reke te kanganga.	
370	These tactics may require a thorough review of what security events should be logged to provide cybersecurity state awareness, how a customer may configure logging, for what time period logs are retained, how log integrity and storage are protected, and how logs can be analyzed.	Anga aikai a kainnanoa ae ana rinanoaki bwa tera bwai ake a riki ni irekereke ma te kamano ae a riai n tauaki mwia ibukin katauraoan katauraoi n aron kamano nte intanete, aron te katitamwa n karaoi tau ni mwin rinnako, ao manin kawakinaia, ao manra ae ana kawakinaki raoi iai, ao ai aron kabwaranakoaia.	
371	In some cases, the review may suggest the need for a refactoring of the application's log management architecture to help make them actionable and at a cost that works for the manufacturer.	N tabetai, ao mwin rinanoaia a kona ni kaota kainanoan aron tein barongaan aron tauan mwin rinnako aonga ni kona ni karaoaki nte boo ae raoiroi irouia taan karaobwai.	
372	Working with incident response (IR) experts can increase the chances that the logs will be useful to investigators in the field.	Mwakuri ma bwakuaku n totokoan kanganga (IR) e kona ni kakerakea anangan bwai n taumwin rinnako bwa ana bongana ibukia taan kakae nte rabakau anne.	
373	See the section on SIEMs.	Noora te mwakoro iaon SIEM.	
374	**[1}Eliminate hidden taxes.**	**[1}Kakeai karekemwane ake a karabaki.**	
375	{1]Publish a commitment to never charge for security or privacy features or integrations.	{1]Boretia are mai nanom ae ko aki kona n tangira te mwane ibukin kamano ke anga ni karaba ke anga ni katomatoma.	
376	For example, within the larger scope of identity and access management (IAM), there are services called single sign-on (SSO) services.	Te kabotau, n aron taran riki aron barongaan kinakim ao rinim (IAM), iai taian tieweti ae aranaki bwa teuana angan-rinim (SSO).	
377	Some manufacturers charge more to connect their system to a SSO service (sometimes referred to as an identity provider).	Tabeman taan karaobwai a kainanoi kabwakamwane riki ngkana kona toma ma aia SSO tititem tieweti (aranaki n tabetai bwa taan katauraoi aron kinakim).	
378	This "SSO tax" means that good identity and access management is out of reach for many SMOs, preventing them from achieving a strong security posture.	Te "SSO karekemwane" nanona bwa barongan kinakim ao rinim a tikiraoi ao aki kona n roko iai SMO, aei are e totokoia bwa ena reke irouia te kamano ae korakora.	
379	Some services charge more to enable MFA for users.	Tabeua tieweti a bobuaka riki ngkana ana kamaua MFA ibukia taan kabongana.	
380	**[1}Security should not be priced as a luxury good but considered a customer right.**{2]	**[1}Te kamano tiaki te karaka aro, ao a riai n taraki katitamwa bwa inaomataia.**{2]	
381	**[1}** {2]Some manufacturers have argued that few customers request these features, and they cost more to maintain.	**[1}** {2]Tabeman taan karaobwai a kauntaeka man taku bwa ti tabeman katitamwa aika bubuti te kamano, ao a nang bobuaka.	

382	These arguments ignore the fact that few customers will call to complain or bargain, not all customers actually understand what the benefits of these features are, and that all features cost something to maintain.	Kauntaeka aikai a katinanikua te koaua ae ti tabeman katitamwa aika a tatarebonia ni kan buokaki, tiaki nanona bwa katitamwa ni kabane a oota n aron kabwaia ake ana reke man bwain karaobwai aikai, ao kai are bwain nako karaobwai a bane ni iai booia ngkana a kakabonganaaki.	
383	Yet we don't see many manufacturers charging extra for availability or data integrity.	Ma kae ti aki nonoria taan karaobwai bwa ana tangiri kabwakamwane ibukin tatauraoin ke nakoraoin aia rongorongo.	
384	The costs to support those key attributes are built into the price all customers pay, much like the costs to include seatbelts, collapsible steering columns, and airbags that save lives in accidents.	Boon boutokan kamano aikai irouia taan karaobwai a bane n rin nte boo are kaboa iai te katitamwa, bon aekakin raoi are boon te kaa e airi ma boon te roo, te bwe ae ririnnako, ao te katibu a bane ni kakaokoro booia ao a kamano n tain kanganga.	
385	**[1}Embrace open standards.**	**[1}Butimwaei aroaro aika bwainaki nte aonnaba.**	
386	{1]Implement open standards, especially around common network and identity protocols.	{1]Iri nanon aroaro aika bwainaki nte aonnaba, riki ngkana e rekereke ma katomatoma ao aron kinakim.	
387	Avoid proprietary protocols when open standards are available.	Katinanikui kaetieti ake a kaboaki ngkana iai ake a bwainaki nte aonnaba.	
388	**[1}Provide upgrade tooling.**{2]	**[1}Katauraoi kabouan bwai ni buobuoki.**{2]	
389	Many customers are reluctant to adopt the latest version of the product, including deploying newer and more secure features like secure network connections.	Angia katitamwa a rawa n kabonganai rinanin karaobwai aika boou, ao kamanenan bwai ni kamano aika boou ibuki te katomatoma.	
390	Software manufacturers can increase customer adoption of new upgrades by providing tooling to help reduce uncertainty and risk.	Taan karaoi kanoan kombiuta a kona ni karakai mwaitia katitamwa aika kabonganai kabou man katauraoan bwai ni ibuobuoki ake a kauarerekei kanganga ao raraoma.	
391	Offer free licenses for customers to test upgrades and patches in a test environment as a way to motivate customers.	Anga raitinti n akea booia n tuoi kabou ao bono raran nte tabo n tutuo bwa am ang ani kaungai nanoia am katitamwa.	
392	**PRINCIPLE 2:**	**KORA NI KAETI 2:**	
393	**[1}** {2][3}Embrace Radical Transparency and Accountability{2]	**[1}** {2][3}Butimwaea te kakirati ao te Onimakinaki{2]	
394	**[1}EXPLANATION**{2]	**[1}KABWARABWARANA**{2]	
395	Software manufacturers should pride themselves in delivering safe and secure products, as well as differentiating themselves from the rest of the manufacturer community based on their ability to do so.	Taan karaoi bwain nanon kombiuta a riai ni kamoaia n aron karokoan karaobwai aika tau man mano, ao ni kaburaia nakoia raoia ni karaobwai ni botona aia kamoamoa iaon aia konabwai ni karaoi nanon aikai.	
396	Let's address a common concern about transparency.	Tia nako n kaitarai tabeaianga ibukin te kakirati.	
397	When practitioners discuss radical transparency, there is a tendency for the conversation to get bogged down in a concern that they are providing a "roadmap for attackers."	Nte tai are taan mwakuri karaobwai a maroro akini aron te kakirati, ao iai te kantaninga ae ena aki bo ma aongina iaan te raraoma ae e kona naba ni katauraoi "mwaben kawai ibukia taan tokobito"	
398	However, the overwhelming evidence is that attackers are doing just fine without such roadmaps, and such concerns should take a back seat to transparency that benefits direct customers, indirect customers, supply chains, and the entire software industry.	E ngae n anne, ma e nang tiraua bwaai ni kakoaua ae taan tokobito akea aia kanganga ngkana akea mwaben kawai aikai, raraoma aikai a riai ni kakerikakaki nako akun te kakirati are a mabiao iai katitamwa ikai, ao katitamwa i kiraroa, taan karaobwai, ao ai bon nikabake rekereken te waki ni karaobwai aei.	
399	Transparency helps the industry establish conventions—in other words, what "good" looks like.	Te kakirati e buoka aroia nikabane rekereken te waki ni karaobwai aei ni katei bobotaki—ti kona ni kangai aio aron tarakin te "tamaroa".	
400	It helps those conventions change over time in response to customer needs, changes in threat actor tactics or economics, or technology	E bubuoki naba bobotaki bwa ana bitaki n taina ni kaitara kainnanoia katitamwa, bibitaki n aron aron aia kumeto kamwarua ke kaubwaia, ke	

	evolution.	bibitakin rabakau aika boou.	
401	Transparency helps manufacturers with fewer resources learn from those with more mature and capable resources.	Te kakirati e buobuoki nakoia taan karaobwai ake a karako aroia n reirei mairouia ake a mwatai ao n tau kaubwaia.	
402	Conversations about information sharing should expand beyond real-time threat indicators, to include the elements below.	Maroro ibukin tibwatibwan rongorongo a riai ni karababaki iaon kanikinaean kanganga aika-ngkai, ao ni kairi bwaai aika i nano.	
403	Transparency forces decisions around security to be made early in the development process, and to be a continuous activity of business leaders as well as engineers and security professionals.	Te kakirati e kaumaki iango ibukin kamanomano bwa ana karaoaki moa imwain babarongan te karaobwai, ao ena reitinakoaki bwa tabeia taan kairiri nte bitiniti ni ikotaki ma intinia ao taan rabakau n aron te kamanomano.	
404	Transparency builds accountability into the product.	Te kakirati e katea te onimakinaki nakon te karaobwai.	
405	A note on the choice of the adjective "radical" in front of "transparency."	Taeka ni kauring iaon kabonganan te taeka ae "akea waewaeana" bwa ena memena imwin "kakirati."	
406	Today, it is uncommon for software manufacturers to publish information about how they develop and maintain software and how they mature their programs using data over time.	N taai aikai, ao ea rang bwainaki ae taan karaoi nanon kombiuta a boreti rongorongon ni kabane ibukin aroia n karioi ao bwain nanon kombiuta ao aroia naba ni ka mwataii aia burokuraem man kabonganan rongorongo.	
407	In the software industry, few manufacturers offer guided tours of how they design their software.	N tabo ni karao bwain nanon kombiuta, ao taan karaobwai tabeua a karaoi neweaban aroia ni mwakuri aia karaobwai.	
408	There are few opportunities for software manufacturers to see how peer organizations structure their SDLC programs, and how those programs hold up in the customer environments against real attackers.	E karako anga irouia taan karao bwain nanon kombiuta n noori aia anga raoia ni katea aia SDLC burokuraem, ao aron matoan burokuraem akanne n aia otabwanin katitamwati ngkana a roko taan tokobito.	
409	The collective industry would benefit from more information sharing on topics such as strategies to measure the cost of security defects and to eliminate classes of vulnerability.	Nikabane nake a rekereke ma te waki ni karaobwai ana bon mabiao man tibwakin riki rongorongo n aron aia ang ani warebwaia boon memeren karaobwai ao boon kamaunan rinanin memere nte karaobwai.	
410	As a result of these common practices, every software manufacturer must learn how to deal with product security on their own.	Mwiin taian waaki aikai, ao nikabane taan karaoi bwain nanon kombiuta a riaia ni bwaati aroia ma memeren karaobwai I bon irouia.	
411	Perhaps by not placing a luxury tax on security features, safety and security therefore becomes a cost center rather than a profit center, and companies would benefit by lightening the load through collaboration and transparency.	Ngke arona bwa akea te karekemwane ni karaka aro man tein kamano, maurim ao manom ana riki bwa te tabo ni kabanemwane ae riai ao tiaki te tabo ni karaka mwane, ao kambwana ana mabiao man bebeten uotaia rinanon te reitaki ao te kakirati.	
412	We want to focus on the tactics that will materially accelerate the evolution of the software industry.	Ti kan katurua ara taratara iaon aanga aika ana kabirimwaka bibitaki nakon te anga ni karikirake aio.	
413	We can no longer afford to make opportunistic, incremental improvements.	Tia aki kona ni tataningai aroaro aika aonikai ao katamaroa aika uarereke.	
414	If we are to collectively overcome the threats posed by intelligent and adaptive adversaries, we must embrace levels of transparency that will feel uncomfortable today, but that will drive the industry forward.	Ngkana ti kan bane n tokari nako kakamaku mairouia kaitarara aika wanawana man bibiti aroia, ao ti riai ni butimwai rinanin kakirati aika ana aki tiaki mwengaraoi iai nte bong aei, ma ana bwena ara waki ni karirake aei nako moa.	
415	There are manufacturers today who embody some of these secure by design principles.	Iai taan karikirake nte bong aei ake a tia ni karabwatai tabeua mai buakon kainibaire ibukin te kamano man karaoaia.	
416	As William Gibson said, "the future is already here, it's just not very evenly distributed."	N aron are taekinna William Gibson, "ea roko kabwaiara, ma e aki nang tibwatibwaki raoi."	
417	**[1}Radical transparency will help distribute that information and**	**[1}Kakirati aika akea waewaeaia ana buoka aron tibwatibwan**	

	benefit the defenders more than our adversaries.{2]	**taian rongorongo ao taan kamanoira ana mabiao riki nakoia aiara.**{2]	
418	Transparency can do more than help peer organizations mature their SDLCs.	Te kakirati e kona riki ni buokia raora ni karaobwai ni kanakoraoi aia SDLC.	
419	Prospective customers and investors can learn more about the investments and tradeoffs manufacturers have made, and the security posture those investments have created for customers.	Ara katitamwa ao taan karinimwane a kona n reiakinia aron te karinimwane ao aia anganano taan karaobwai ake a tia ni karaoi, ao ai tein kamanoaia ara katitamwa ake a tia n reke man kabanemwane akanne.	
420	Manufacturers who embrace radical transparency will give customers information to help them make purchasing decisions not just on price and features, but on security as well.	Taan karaobwai ake a butimwai kakirati aia aki waewaeaki a angania katitamwa rongorongo ibukin aron aia bobwai tiaki ti man boon bwaai ao teia, ma iaon manoia naba.	ana n
421	As hard as organizations work to secure their supply chain and their SDLC, companies have had their builds processes compromised in the recent past.	Mwakurian kamatoan kamano irouia kambwana ibukin kamanoan aia taan karaoi aia bwai ao aia SDLC, kambwana nako a tia n tokobitoaki n taai aika nako.	
422	Embracing radical transparency should lead to public disclosure of the attack as well as the improvements the company made to prevent and detect future attacks.	Butimwaean kakirati aika akea waeaia a riai ni kairira nakon totokoan ao nooran tokobito n taai aika i mwaira.	
423	That form of information sharing will help other organizations learn without having to suffer the same fate.	Te aekaki n tibwa rongorongo aio ni buokia kambwana ake tabeua ni bwaati aroia n aki manga reke n aekakin kanganga aikai.	ena
424	**DEMONSTRATING THIS PRINCIPLE**	**REIAKINAN TE KAINIBAIRE AIO**	
425	To demonstrate this principle, software manufacturers should take steps including the following:	Ibukin reiakinan te kainibaire aio, ao taan karaoi bwain nanon kombiuta a riai n toui mwaneka aikai:	
426	**TLP:CLEAR**	**TLP:CLEAR**	
427	**SECURE BY DEFAULT PRACTICES**	**WAAKI NI KAMANO MAN TEINA**	
428	**1.[1]Publish aggregate security relevant statistics and trends.**	**1.[1]Boreti kabwaninan aron kamano waare aika riai ao taian bitaki.**	
429	[1}Example topics include MFA adoption by customers and administrators and use of unsafe legacy protocols.{2]	[1}Katoto iaon bwaai aika ana maroroakinaki bon bwainakin MFA irouia katitamwa ao taan kabongana ao kabonganan aanga ni kawai aika aki mano.{2]	
430	**2.[1]Publish patching statistics.**	**2.[1]Boreti waaren bonobono.**	
431	[1}Detail what percent of customers are on the latest version of the product, and what you are doing to make updates easier and more reliable.{2]	[1}Kababanea bwa iraua mwaitia katitamwa ni katoa tebubua aika a toka iaon tein karaobwai aika boou, ao tera ae ko karaoia ibukin kabebetean kaboou bwa aonga ni bebete ao n onimakinaki riki.{2]	kaboui
432	**3.[1]Publish data on unused privileges.**	**3.[1]Boreti rongorongo iaon mabiao aika aki kabonganaki.**	
433	[1}Publish aggregate information on excessive permissions across your customer base as well as the nudges and other changes to the product you are making to reduce the customers' attack surfaces.	[1}Boreti kabwaninan rongorongo iaon rakanakon kariaia irouia am katitamwa nako ni ikotaki ma kaungaunga ao bitaki tabeua nakon te karaobwai ae ko karaoia ibukin kauarerekean te tokobito.	
434	These unused privileges are likely to be good candidates for administrator alerts, like seatbelt chimes.{1]	Mabiao aika aki kabonganaki aikai a kona n riki bwa taian bwai ni kauring aika tikiraoi nakoia taan kabongana, kanga aekakin are te roo nte ka.{1]	
435	CISA | NSA | FBI | ACSC | CCCS | CERT NZ | NCSC-NZ | NCSC-UK | BSI | NCSC-NL	CISA | NSA | FBI | ACSC | CCCS | CERT NZ | NCSC-NZ | NCSC-UK | BSI | NCSC-NL	
436	NCSC-NO | NÚKIB | INCD | KISA | NISC-JP | JPCERT/CC | CSA |	NCSC-NO | NÚKIB | INCD | KISA | NISC-JP | JPCERT/CC | CSA |	

Checked

	CSIRTAmericas	CSIRTAmericas	
437	**TLP:CLEAR**	**TLP:CLEAR**	
438	**1**	**1**	
439	**2**	**2**	
440	**3**	**3**	
441	**4**	**4**	
442	**TLP:CLEAR**	**TLP:CLEAR**	
443	[1]	[1]	
444	**SECURE PRODUCT DEVELOPMENT PRACTICES**	**ARON BARONGAN KARAOBWAI AIKA MANO**	
445	**[1}Establish internal security controls.**	**[1}Karioi oin am anga n taratarai aron kamanomano.**	
446	{1]Many companies have seen the benefits of moving their data to cloud providers.	{1]A mwaiti kambwana aika a tia n noori mabiao man kamwaingan aia rongorongo nakon tain tiewa.	
447	Now those cloud providers become the target of attackers.	Ao ngkai taan katauraoi tiewa akanne a manga riki bwa aia takete taan tokobito.	
448	Software as a Service (SaaS) providers should publish statistics of their internal controls.	Bwai nanon kombiuta a riki bwa tieweti (SaaS) ao taan katauraoia a riai ni boreti waaren oin aia anga n taratarai.	Bwain add
449	For example, SaaS providers should publish statistics on their internal deployment of [1}[2}phishing-resistant MFA,{3]{4] like Fast Identity Online (FIDO) authentication.	N aron te katoto, taan katauraoa SaaS a riai ni boreti waare ibukin aia anga n kaotinako te[1}[2}totokoan-tokobito nte imeri MFA,{3]{4] n aron Kinakim Aonrain ae Tawe (FIDO) kinakim raoi.	kaotinakoa delete
450	Ideally, they should be able to say that no staff member can access customer or other sensitive data without authenticating via phishing-resistant MFA.	Ni bon arona, a riai ni kona n taekinna ae akea aia taan mwakuri ae kona ni kumea te katitamwa, ke rongorongona aika kamanoaki n akean kinakim raoi rinanon totokoan-tokobito nte imeri MFA.	a
451	**[1}Publish high-level threat models.**	**[1}Boreti aron barongan kakamaku aika raka-aroia.**	
452	{1]Secure by design products start with written threat models that describe what the creators are trying to protect and from whom.	{1]Karaobwai aika mano man karaoaia e moanaki karaoaia ma barongan kakamaku aika raka aroia aika kabwarabwarai bwai ake a katai ni kamanoi taan kario ao mai iroun antai.	
453	Effective threat models are informed by the way intrusions happen in the wild, and should cover both the enterprise and development environments, as well as the way the software manufacturers intend for it to be used in customer environments.	Barongan kakamaku aika tau a karekei moa rongorongo n aron mwakurin tokobito nte wild, ao e riai n rotii kambwana ao tabo ni babaronga, ni ikotaki ma te aro are taan karaoi bwain nanon kombiuta a tia ni kataua ibukin kabonganana irouia katitamwa.	otabwanin
454	**[1}Publish detailed secure SDLC self-attestations.**	**[1}Boreti am-kakoaua ibukin SDLC aika matata ao ni mano.**	
455	{1]Manufacturers following NIST SSDF, or other similar frameworks are actively working towards a mature software development lifecycle.	{1]Taan karaobwai ake a iri NIST SSDF, ke aron tein karaobwai ake tabeua, a kakamwakuri ni mwakuri nakon aron karaon bwain nanon kombiuta aika matoa.	
456	Publishing a self-attestation of which controls the manufacturer has enacted, and for which products, would demonstrate a commitment to adhering to these best practices and provide an increased level of confidence to their customers.	Boretian am-kakoaua ake tarataraia naba taan karaobwai ea kabonganaki, ao ibukin te karaobwai ae enga iai, ena kaota aron te waaki ae nanonaki ibukin karaoan nanon kawai aika tamaroa ao katauraoaia katitamwa bwa ena raka onimakinaia irouia. aia katitawma	add to end
457	Other certification schemes include the Israel Cyber Supply Chain Methodology, for instance.	Kawain riki karioan kinakim bon Aroia taan Karaobwai nte intanete i Iteraera, kanga te kabotau.	
458	**[1}Embrace vulnerability transparency.**	**[1}Iri nanon kakirati nte memere.**	
459	{1]Publish a commitment that will ensure that identified product	{1]Boretia are mai nanom bwa ena kakoauaki ae memere nte karaobwai	

	vulnerabilities will be published as CVE entries that are correct and complete.	are a kuneaki ana boretiaki ibuakon CVE ake a eti man tabwanin taekaia.	Checked
460	That's especially true for the Common weakness enumeration field that identifies the root cause of the vulnerabilities.	Aei e nang koaua riki n aron Warebwaian memere aika okioki are e kaotii naba boton rikin taian memere.	
461	The more correct and complete the public CVE database is, the more the industry can track how products are becoming more secure, and which classes of vulnerabilities are most prevalent.	Rakan etin ao tabwaninin bokin CVE ae a roko iai aomata ni kabane, ai bon rakan naba ana anga te botaki ni karikirake aei ni kona n noria bwa te aro ra ae a mano iai karaobwai, ao anga rinanin memere aika a okioki.	
462	However, beware of the temptation to count CVEs as a negative metric, since such numbers are also a sign of a healthy code analysis and testing community.	Ma, tai kaririaki ao ni wareki CVE bwa te ware ae katerea te bwai ae buakaka, aio bukina bwa waare aikai a kaota naba aron raoiroin tirobaean te burokuraem ao tikiraoia taan tirobaeia.	
463	As manufacturers implement a secure by design philosophy, it's possible that at first their raw CVE count will go up due to more comprehensive discovery and remediation of vulnerabilities in existing code.	Ngkai a tabe taan karaobwai ni mwakuria aron karaoana man kabonganan taeka n rabakau nte kamano man karaoana, e kona ni kerake aia moan ware nte CVE ngkai a karaoi kanoan kukune ake a bwakanako n aia anga ae tuoi memere n taai aikai.	
464	Manufacturers should publish analysis of past vulnerabilities, including any patterns and measures that were taken to address the entire class of vulnerabilities.	Taan karaobwai a riai ni boreti tirobaean memere ake rimoa, ni ikotaki ma taian kawai ao baeten ao anga ake a karaoi n totokoi karinanin nako te memere.	
465	For example, if a large percentage of a company's CVEs were related to cross-site scripting (XSS), documenting the root cause analysis, response (such as shifting to web template frameworks that prevent XSS), and results would signal to customers that they will not be victimized by a class of vulnerability for which mitigations have been understood for decades.	Te kabotau, ngkana e mwaiti man ikotan ana CVE te kambwana ae a rekereke ma aron bitakin-uebutiati (XSS), tauan mwin tirobaean boton kanganga, aron tokoana (n aron bibitan tein te karaobwai are totokoa te XSS), ao ena kaotia nakoia katitamwa ae ana aki kona n aonikaiaki man karinan ni memere ake iai bwainaoraki ibukia a tia n ataki inanon tebwi tabun te ririki.	
466	**[1}Publish Software Bills of Materials (SBOMs).**	**[1}Boreti Bwain Kanoan Nanon am Karaobwai: (SBOMs).**	
467	{1]Manufacturers should have command of their supply chains.	{1]Taan karaobwai a riai n taui taekan aia kanoan nako aia karaobwai.	ia taan
468	Organizations should build and maintain SBOMs \[2] for each product, request data from their suppliers, and make SBOMs available for downstream customers and users.	Boboti a riai ni katei ao ni kawakina raoiroin SBOM \[2] n aia karaobwai nako, bubuti rongorongo mairouia taan karaoi kanoan aia karaobwai, ao angania katitamwa ao taan kabongana taian SBOM.	
469	This will help demonstrate their diligence in understanding the components they use in the creation of their products, their ability to respond to newly identified risks, and can help customers understand how to respond if one of the modules in the supply chain has a newly found vulnerability.	Aio ena ibuobuoki n aron kabwaranakoan koauan aia atatai ni bwai ake a kabonganai ni karaoan aia karaobwai, aia konabwai n totokoi kanganga aika boou, ao e kona ni buokia katitamwa n atai aroia n totokoi kanganga ngkana teuana kanoana iai memere aika kuneaki iai.	
470	For reference, Japan's Ministry of Economy, Trade, and Industry (METI) has published [1}[2}"Guide of Introduction of Software Bill of Materials (SBOM) for Software Management."	Ibukin ritioti ao, Ana Tabo ni Mwakuri Tiaban ibukin Kaubwai, Iokinibwai ao Karikirake (METI) ea tia ni boreti {1][2}"Kairi ibukin Barongan Katerean Kanoan Nanon Karaobwai." (SBOM)	reburenti add
471	{1]{2]Transparency should extend to firmware in embedded devices and the data and models used in AI/machine learning (ML).	{1]{2]Te kakirati e riai n roti bwain nanon kombiuta ake a nim inanon bwain mwakuri te rongorongo ao tein kabonganan AI/reiakinan mitiin (ML).	ao
472	[1}Beyond assisting in purchasing decisions {2]and operational capabilities, SBOMs play an important role in the infrastructure to detect and respond to malicious supply chain attacks.	[1}Irarikin riki te buobuoki ni karaoan iango ni bobwai{2]ao konabwaina n ana mwakuri, taian SBOM iai tabeia ae bongana inanon te kateitei ni kakae ao n totokoi bwain nanonkaraobwai aika kaikoaki.	bobwai {2]ao nanon karaobwai

473	**[1}Publish a vulnerability disclosure policy.**	**[1}Boreti kainibaire ibukin kaotan memere.**	
474	{1]Publish a vulnerability disclosure policy that (1) authorizes testing against all products offered by the manufacturer and conditions for those tests, (2) provides legal safe harbor for actions performed consistent with the policy, and (3) allows public disclosure of vulnerabilities after a set timeline.	{1]Boreti kainibaire ibukin kaotan memere aika (1) anga te kariaia ibukin tuoan karaobwai ake a nikiraki irouia taan karaobwai ao kainibaire ibukin tutuo akanne, (2) katauraoi naba nnen mwakuri ake a karaoaki ao n rinanon te kainibaire, and (3) ao kariaia kaotan memere nakon te botanaomata imwin te tai ae baireaki.	delete
475	Manufacturers should perform root-cause analysis of discovered vulnerabilities and, to the greatest extent feasible, take actions to eliminate entire vulnerability classes.	Taan karaobwai a riai ni karaoi mwamiran boton-kanganga man memere aika kuneaki ao, nakon aia kabanea ni kona, karaoi mwakuri ni kamaunanakoi karinan ni memere.	
476	See CISA's [1}[2}Vulnerability Disclosure Policy Template{3]{4] for reference language. ana reburenti	Nora CISA [1}[2}Taiboran Kainibaire ibukin Kaotan Memere{3]{4] ibukin burokuraem aika kabonganaaki.	add
477	CISA | NSA | FBI | ACSC | CCCS | CERT NZ | NCSC-NZ | NCSC-UK | BSI | NCSC-NL	CISA | NSA | FBI | ACSC | CCCS | CERT NZ | NCSC-NZ | NCSC-UK | BSI | NCSC-NL	
478	NCSC-NO | NÚKIB | INCD | KISA | NISC-JP | JPCERT/CC | CSA | CSIRTAmericas	NCSC-NO | NÚKIB | INCD | KISA | NISC-JP | JPCERT/CC | CSA | CSIRTAmericas	
479	**1**	**1**	
480	**2**	**2**	
481	**3**	**3**	
482	**4**	**4**	
483	**TLP:CLEAR**	**TLP:CLEAR**	
484	[1]	[1]	
485	**PRO-SECURITY BUSINESS PRACTICES**	**KAWAIA BITINITI AKE A NANONI-KAMANO**	
486	**Publicly name a secure by design senior executive sponsor.**	**Kaotia nakon te botanaomata aran te tia tara aron kamano man karaoaia.**	
487	[1}In many organizations, security (like quality) is delegated to technical teams who have limited ability to make structural changes to dramatically improve the security of the products.	[1}Ni kambwana aika rawata, ao te kamano (n aron tamaroana) a onimakinaki iai taan mwakuria ake iai tokin aia konabwai ni karaoi bitaki nakon tein karaobwai ake a kona n rangi ni katamaroa manon karaobwai.	
488	Publicly naming a top business executive to oversee the secure by design program will transform the security of products into a top-level business concern.{1]	Kaotan aran te tia kairiri mai ieta nakon te botanaomata are ena taraa aron te kamano man karaoana ena bita kamanoan karaobwai bwa ena moan-bwai n ana tabeaianga te bitiniti.{1]	add
489	**Publish a secure by design roadmap.**	**Boretia mwaben kawai ibukin kamano man karaoana.**	
490	[1}Manufacturers should document changes made to their SDLC to improve customer security, including details about field-test reports, actions taken to eliminate entire classes of vulnerability, and other items listed in the other principles.	[1}Taan karaobwai a riai n taumwiinbibitaki ake a karaoi nakon aia SDLC ni katamaroa manoia katitamwa, n aron taekan nako ribotinakin mwiin kakae nte-marae, mwakuri ake a karaoaki ibukin kamaunanakoan rianin memere, ao bwai riki ake a koreaki inanon kainibaire ake tabeua.	tau mwiin bibitaki rinanin
491	As in the case of quality improvement efforts, security improvement programs have distinct phases of planning, control, and improvement.	Kanga n ai aron katamaroan mwakuri ni katamaroa, mwakuri ni katamaroai burokuraem ni kamano iai karinanin tein aron bairean, tauan mwiin, ao improvement.	katamaroa
492	In the spirit of showing rather than telling, publishing the roadmap and the details behind these phases will build confidence that the products are secure by design.	Bukina bwa e aanaki n te tamnei are karaoia, ma tai tataekinna, ao boretian mwaben kawai aika bwarabwarai karinan ni karaobwai aikai ana karika te aki nanokokoraki bwa te karaobwai a mano man karaoana.	kabwarabwarai e
493	After achieving meaningful progress manufacturers can detail them in	Imwin reken te tamaroa ae bongana ao taan karaobwai a konaa ni	

	transparency reports.	kabwarabwarai raoi ninanon riboti ni kakirati.	
494	Doing so not only demonstrates a commitment to secure by design principles but can inspire others to adopt similar programs by showing an existence proof.{1]	Karaoan aio e aki ti kaota te taua n nano nakon kainibaire ibukin kamano man karaoana ma e kona ni kauekeia tabemwang bwa ana irii aekakin burokuraem aikai man kaotan koaua aika iai rabwataia. {1]	
495	**Publish a memory-safety roadmap.**	**Boreti mwaben kawai ibukin kamano man rinnakoan-ururing.**	
496	[1}Manufacturers can take steps to eliminate one of the largest classes of vulnerability by migrating existing products and building new products using memory safe languages.	[1}Taan karaobwai a kona n toui mwaneka nakon kamaunanakoan teuana karinanin te memere ae bubura man kamwaingan karaobwai aika iai ao karaoan karaobwai aika boou man kabonganan burokuraem aika mano man rinnakoan ururing.	
497	While this may not be possible in all cases, manufacturers can consider developing application wrappers in memory safe languages instead of re-writing entire applications.	Ngkai aei e kona n aki mwakuri n tabetai, taan karaobwai a kona ni iangoi karaoan karaobwai aika bon taui mwiia man kabonganan burokuraem aika mano man rinnakoan ururing n onea mwiin manga-korean karaobwai mai moana.	
498	This can also include how manufacturers are updating hiring, training, code review, and other internal processes, as well as ways they are helping the open source community do the same.{1]	E konaa aio naba ni kaira aroia taan karaobwai ni kaboou aron kateirake, kataneiai, rinanoan code, ao aia waaki i bon irouia, ni ikotaki ma anga ibukin buokan te ibukin karaobwai ake aki kaboaki ni karaoa ae aekakin aei.{1]	kaboui taetaen karaobwai delete
499	**Publish results.**	**Boreti bwai ake a reke.**	
500	[1}While updating their SDLC to embody a secure by design philosophy, organizations will find quick wins, more resource intensive wins, and some unexpected setbacks.	[1}Inanon tain kakabouan aia SDLC ibukin karabwataan te philosophy ibukin kamano man karaoana, kambwana a kona ni kunei katamaroa, katamaroa aika kainanoi ritioti, ao tabeua ananga n totoko aika aki kantaningaki.	rabakau ni karaobwai
501	By presenting their internal successes and roadblocks, the entire industry can learn from the results.{1]	Man kaotan aia tokanikai ibon irouia ao ananga n totoko, te botaki ni karikirake ae bwanin e kona n reireinna man mwiin karaobwai.{1]	i bon
502	CISA | NSA | FBI | ACSC | CCCS | CERT NZ | NCSC-NZ | NCSC-UK | BSI | NCSC-NL	CISA | NSA | FBI | ACSC | CCCS | CERT NZ | NCSC-NZ | NCSC-UK | BSI | NCSC-NL	
503	NCSC-NO | NÚKIB | INCD | KISA | NISC-JP | JPCERT/CC | CSA | CSIRTAmericas	NCSC-NO | NÚKIB | INCD | KISA | NISC-JP | JPCERT/CC | CSA | CSIRTAmericas	
504	**TLP:CLEAR**	**TLP:CLEAR**	
505	[1]	[1]	
506	**PRINCIPLE 3:**	**KORA NI KAETI 3:**	
507	**[1}** {2][3}Lead from the Top{2]	**[1}** {2][3}Kairiri mai eta{2]	Eta
508	**EXPLANATION**	**KABWARABWARANA**	
509	While the overall philosophy is called "secure by design," the incentives for customer safety begin well before the product design phase.	E ngae ngke te taeka n rabakau ae kabuta e aranaki bwa te "kamano man karaoana," anga n anainano ibukin kamanoaia katitamwa e moanaki imwain riki tain katameian te karaobwai.	
510	They begin with business goals and implicit and explicit objectives and desired outcomes.	E moanaki man ana kouru te bitiniti ao takete ake a taekinaki ao ake aki taekinaki ao ai bwai aika kantaningaki.	
511	Only when senior leaders make security a business priority, creating internal incentives, and fostering an across-the-board culture to make security a design requirement will they achieve the best results.	Bon ti taan kairiri ake i eta ae a karaoa te kamano bwa aia moanibwai, ni karaoi oin aia anainano, ao ni karaoa te aroaro ae akea-te-katinanikuaki ao karaoan te kamano bwa irian ana waaki ni karaobwai ao ana kona ngkanne n karekea te karaobwai ae te kabanea n tamaroa.	

512	While technical subject matter expertise is critical to product security, it is not a matter that can be solely left to technical staff.	E ngae ngke rabakauia intinia e kakawaki ibukin karaobwai ni kamano, ma ena aki riai ni katukaki ti nakoia intinia.	
513	It is a business priority that must start at the top.	Bon ana moanibwai te bitiniti ae e riai ni moanaki karaoana mai eta.	
514	Some people have wondered if a software manufacturer is embracing the first two principles and producing meaningful artifacts, is the third principle necessary?	Tabeman aomata a mimi ngkana taan karaobwai a butimwaai kora ni kaeti ake uoua mai eta ao ni katiai karaobwai aika tamaroa, iai ngkanne kakawakin te ka teniua ni kora ni kaeti?	
515	How a company establishes its vision, mission, values, and culture will affect the product, and those elements have a heavy component at the top.	Aron te kambwana ni kawenei ana taratara, kawaina, baika kakawaki, ao katei ana rot ate karaobwai, ao bwai akanne a rangi n rekereke na kain eta.	rota te m
516	We see this in other industries that have made dramatic improvements in safety and quality.	Ti nora aio n waki ni karekemwane ake tabeua ake a tia ni karaoi karirakean te kamano ao te tamaroa.	
517	Noted quality expert J.M. Juran wrote:	Te tia rabakau iaon te tamaroa ae kinaki J.M.Juran e korea:	
518	**We believe that security is a sub-category of product quality.**	**Ti kakoaua ae te kamano e mena-iaan tamaroan karaobwai.**	
519	[1}When security and quality become business imperatives rather than technical functions left solely to technical staff, organizations will be able to respond to the security needs of their customers more quickly and efficiently.	[1}Ngkana arona bwa kamano ao katamaroa a moanibwai nte bitiniti n onea mwin tabeia intinia ake a bon ti kakaraoia intinia, ao kambwana ana kona n karaoi kainnanoia katitamwa ae te kamano nte tai ao tawe man kakaitia.	e
520	Moreover, investing the necessary resources to ensure that software security is a core business priority from the beginning will reduce the long-term costs of addressing software defects–and in turn, lower the national security risks.	Irarikin anne, karinan ritioti ni kakoaua ae karaoan bwain nanon kombiuta bon te boton te karikirake ae ena moanibwai mai moana ena kauarerekea boon karaoan memeren karaobwai-ao i mwina, ena kauarerekea kanganga ni kamano.	delete
521	In the same way that leadership teams have implemented corporate social responsibility (CSR) programs, there is growing awareness that corporate boards, including those of software manufacturers, should take a more active role in guiding cybersecurity programs.	N aron naba aia tiim taan kairiri ake a tia ni karaoi burokuraem ibukin tabeia kambwana irouia aomata (CSR), iai te rikirake nte ataibwai ae kain te baba n tararua, ni ikotaki ma nake a kakaraoi bwain nanon kombiuta, a riai ni karaoi riki tabeia ni kairi burokuraem ni kamano nte intanete.	
522	The term corporate cyber responsibility (CCR) is sometimes used to describe this emerging idea.{1]	Te taeka ae tabeia kambwana te kamano nte intanete (CCR) e kabonganaki n tabetai ibukin kabwarabwaran te iango ae rikirake aei.{1]	
523	***Attainment of quality leadership requires that the upper managers personally take charge of managing for quality.***	***Reken te kairiri ae tamaroa e kainnanoia manatia ake i eta bwa ana taua taekan barongan te katamaroa.***	
524	***In companies that did attain quality leadership, the upper managers personally guided the initiative.***	***Ni kambwana ake a reke irouia te kairiri ae tamaroa, manatia ake i eta a kaira te katabwena aei.***	
525	***I am not aware of any exceptions. \[3]***	***I aki atai ae iai ae kaokoroaki. \[3]***	
526	**DEMONSTRATING THIS PRINCIPLE**	**REIAKINAN TE KORA NI KAETI AEI**	
527	To demonstrate this principle, software manufacturers should take steps including the following:	Reiakinan te kora ni kaeti aei, ao taani karao bwain nanon kombiuta a riai n toui mwaneka ni ikotaki ma aika i nano:	
528	**Include details of a secure by design program in corporate financial reports.**	Kairi rongorongon nako te burokuraem ae te kamano man karaoana ma ribotin mwaanen te boboti.	
529	[1}If the manufacturer is a publicly traded company, add a section in each annual report devoted to secure by design efforts.	[1}Ngkana te kambwana e toka iaon te mwakete ni iokinibwai, karaoa teuana te iteraniba ni katoa ririki ae boboto ibukin anga ni kamano man karaoaia.	
530	It is common for automobile annual financial reports to include sections on driver and passenger safety, including information about centralized	E rangi ni bwainaki irouia taan karao kaa n ribotin aia mwane ni katoa ririki bwa ana kairi iteraniba ibukin kamanoaia turaiwa ao bwatintia, a kairi	bwabwainaki

	and distributed quality and safety committees.	rongorongon te komete ibukin tamaroan ao manon aia tiewa ae onoti ao ae tibwatibwaki.	
531	Detailing the secure by design program in a financial report will demonstrate that the organization is linking customer security and corporate financial outcomes and not simply adopting a term in marketing materials because it is in vogue. {1]	Kabwaranakoan te burokuraem ibukin kamano man karaoakina inanon ribotin te mwane ena kaotia ae te kambwana e katoma manon aia katitamwa ma mwin mwanen te kambwana ao e aki ti kamanena te taeka ibukin mwakete bukina bwa e tabangaki taekana. {1]	
532	**Provide regular reports to your board of directors.**	**Katauraoi riboti n taia nakon te baba n tararua.**	
533	[1}Chief information security officer (CISO) reports to corporate boards usually include information about current and planned security programs, threats, suspected and confirmed security incidents, and other updates centered on the security posture and health of the company.	[1}Ana ririboti Mataniwia Aobitia ibukin Kamanoan Rongorongo (CISO) nakon te baba n tararua e rin iai rongorongo ibukin burokuraem ni kamano aika ngkai ao aika babarongaki, kakamaku, raranin kamano aika kataunariaki ao aika a matoa, ao ai rongorongo aika boou aika boboto iaon tein kamano ao marurungin te kambwana.	deacrease space
534	In addition to receiving information about the security posture of the enterprise, boards should request information about product security and the impact it has on customer security.	Irarikin reken rongorongo iaon tein kamanoan te kambwana, baba n tararua a riai ni bubuti rongorongo ibukin manon karaobwai ao arona n roti aron manoia katitamwati.	
535	Boards should not look solely to the CISO, but primarily to other members of company management to drive customer risk down.{1]	Baban tararua ana riai n aki ti tar ate CISO, ma ana taraia riki ana taan kairiri te kambwana ake tabeman ibukin kauarerekean kanganga nakoia katitamwa.{1]	tara te
536	**Empower the secure by design executive.**	**Kakorakora riki te tia kairiri ibukin kamano man karaoana.**	
537	[1}There is a significant difference between an organization where the technical teams have "executive buy-in," and those where business leaders personally manage the customer security improvement process using standard business processes.	[1}There is a significant difference between an organization where the technical teams have "executive buy-in," and those where business leaders personally manage the customer security improvement process using standard business processes.	??
538	The term "executive buy-in" implies that someone had to sell the idea of a customer safety program rather than it being a top-level business goal.	Te taeka ae "kaboan mataniwi-inanoa" te karariki n taetae ae iai ae ena kabonakoa te burokuraem ibukin kamanoaia katitamwa nakon are ena riki kamanoaia bwa te moani-bwai n ana kouru te bitiniti.	
539	This executive must be empowered to influence product investments to achieve customer security outcomes.{1]	Te tia kairiri aei e riai ni kakorakoraki bwa ena kona ni kairi aia iango taan karinimwane ibukin te karaobwai ae ena karekei kamanoaia katitamwa.{1]	
540	**Create meaningful internal incentives.**	**Karaoi anainano nte kambwana aika iai manenaia.**	
541	[1}While being mindful to not create perverse incentives, align reward systems to improve customer security to match other valued behaviors and outcomes.	[1}Ngkai ti bon ataia ae tina aki karaoi anainano aika akea nanoia, kangaraoi aron kaniwanga ake ana katamaroai aron kamanoaia katitamwa ni katitaboa ma aroaro aika raraoi ao mwiin aia mwakuri.	
542	From the secure by design executive to product management, software development, support, sales, legal, and other organizations, weave customer security incentives into hiring, promotions, salaries, bonuses, stock options, and other common processes in the running of the business.	Mairoun te mataniwi nte kamano man karaoana ni karokoa irouia taan babarongai karaobwai, taan karaoi bwain nanon kombiuta, boutoka, taan bobwai, rooia, ao boboti ake tabeua, rarangai anainano ibukin kamanoaia katitamwa rinanon kateirake, bwakabwai, boneti, karinmwane aika raraka, ao ang ariki tabeua n aron kabutan te bitiniti.	anga riki
543	For example, when establishing criteria for promoting software developers, include considerations for improving the security of the product along with other criteria like uptime, performance, and feature improvements.{1]	Te kabotau iai, ngkana a kaweneaki aroaro ibukin kakerakeaia taan karaoi karaobwai ibukin kombiuta, karini iango ibukin katamaroan kamanoan karaobwai ni irianaki ma aron manin maiun tiewa, birimwakan tiewa, ao katamaroan mwakurin karaobwai.{1]	
544	**Create a secure by design council.**	**Katea te kauntira ibukin kamano man karaoana.**	

Checked

545	[1}In some industries, it's common for organizations to create a central quality council, and to embed quality representatives in key divisions or business units.	[1}Tabeua botaki ni karekemwane, ao e nonoraki bwa botaki aikai a karaoa kauntira ibukin katamaroa, ao a rinei kaina man aia tabo ni mwakuri ake a kakawaki riki ke man mangan bitiniti.	N tabeua i mwangan
546	By including both centralized and distributed members, these groups work to improve quality against top level goals while receiving telemetry from deep in the organization.	Man karinaia kain te kambwana ao kain tinaniku, kurubu aikai ana uaia ni mwakuri ni kakerakea te tamaroa n aron kouru mai eta ao a bon rereke naba rokon rongorongo irouia rinanon te ea mai irouia kain te kambwana.	
547	Similarly, a secure by design council would improve security against secure by design goals throughout the organization.{1]	N aron naba aei ao, te kauntira ibukin kamano man karaoaia e katamaroai aron kamanomano man karaoaia ni mwangan nako te kambwana.{1]	
548	**Create and evolve customer councils.**	**Karaoi ao bibiti aia kauntira katitamwa.**	
549	[1}Many software manufacturers have customer councils comprised of customers from different regions, industries, and sizes.	[1}Angia kambwana ni karao bwain nanon kombiuta iai aia kauntira katitamwa ae kaainaki irouia katitamwa, man tabo aika kakaokoro, botaki ni karao bwai, ao buburaia.	
550	These councils can provide a great deal of information about customer successes and challenges in deploying the company's products.	Kauntira aikai a katauraoi rongorongo aika bati ibukin tokanikai irouia katitamwa ao kanganga n aron kaotinakoan ana karaobwai te kambwana.	
551	Structure the council agenda with dedicated topics addressing customer safety, even if it's not currently top of mind for the participants.	Barongai kanoan waan te kauntira ma ianga aika onoti ibukin kaitaran aron kamanoaia katitamwa, e aoria ngkana tiaki moa aia iango.	o
552	Consider where the customer council reports and how to tap participants for insights into the product's security as deployed.	Iangoi bwai ake ana kona n ribotini aia kauntira katitamwa, ao anga n kabonganaia ibukin iango ni kataratara aron kaotinakoan karaobwai	
553	For example, does the council have a bias towards marketing and sales purposes, or product management?	Te kabotau, iai ana tabeitera te kauntira ibukin te mwakete nakin karaobwai ao bukin kabonakoaia, ke aron barongan karaobwai?	ibukin
554	The secure by design executive should help steer these customer interactions and should link them with other elements in this paper, such as field studies.{1]	Te tia kairiri iaon te kamano man teina e riai ni ibuobuoki ni bweni aron reitakia katitamwa ao ni reiti ma bwai tabeua nte beba aei, n aron kamatebwai ma katitamwa.{1]	n
555	**SECURE BY DESIGN TACTICS**	**KAWAI NI KAMANO MAN KARAOANA**	
556	The Secure Software Development Framework (SSDF), also known as the National Institute of Standards and Technology's (NIST's) [1}[2}SP 800-218{3]{4], is a core set of high-level secure software development practices that can be integrated into each stage of the software development lifecycle (SDLC).	Te botaki ae Aron Karaoan Bwain Nanon Kombiuta ae Mano (SSDF), ae ataki n arana ae te Rabwata ibukin Kaeti ao Rabakau aika Boou (NIST) [1}[2}SP 800-218{3]{4], bon ngaai kanoan taian karikirake n te kamano aika raoiroi riki are e na kona ni ikotaki ma Aron Karaoan Bwain nanon Kombiuta (SDLC).	
557	Following these practices can help software producers become more effective at finding and removing vulnerabilities in released software, mitigate the potential impact of the exploitation of vulnerabilities, and address the root causes of vulnerabilities to prevent future recurrences.	Man mwakurian aikai ena buokia taan karaoi bwain nanon kombiuta angania te kona ni kunei ao ni kanakoi memere mai nanon karaobwai ake a kaotinakoaki, taobarai kanganga ake ana riki man tokobitoan memere akanne, ao kakaean boton rikin memere n totokoa manga rikina.	
558	The authoring organizations encourage the use of secure by design tactics, including principles that reference SSDF practices.	Taan anga kariaia nte intanete e kaunga kamanenaakin kawai ni Kamano man Karaoana, n raonaki ma kainibaire ake inanon te SSDF.	a
559	Software manufacturers should develop a written roadmap to adopt more secure by design software development practices across their portfolio.	Taan karaobwai ana koroi ake ana kamanenaaki n te Kamano man Karaoana ake ana taraki bwa kanoan te waki ibukin karikirakean karaobwai.	
560	The following is a non-exhaustive illustrative list of roadmap best practices:	Aikai ngkanne te karinanin mwaben kawai aika-kimototo ibukin	

		karaoana ae tamaroa:	Checked
561	**[1}Memory safe programming languages (SSDF PW.6.1).**{2]	**[1}Ana Taetae te Kombiuta ae Mano (SSDF PW.6.1).**{2]	
562	Prioritize the use of memory safe languages wherever possible.	Moanibwaia kabongana ana taetae te kombiuta aika mana ngkana e kona.	o
563	The authoring organizations acknowledge that memory specific mitigations may be helpful shorter-term tactics for legacy codebases.	Taan anga kariaia a ataia ae bwainaorakian ana ururing te kombiuta a kona I bongana ibukin anga aika-kimototo ibukin karaobwai mgkoa.	ni
564	Examples include C/C++ language improvements, hardware mitigations, address space layout randomization (ASLR), control-flow integrity (CFI), and fuzzing.	Te katoto n aron C/C++ katamaroan taetae,bwain aorakian kombiuta, tokobitoan nnen ana ururing te kombiuta (ASLR), Kakorakoran totoko nakon butin ana waaki te Kombiuta (CFI), ao katamaroa riki.	
565	Nevertheless, there is a growing consensus that adoption of memory safe programming languages can eliminate this class of defect, and software manufacturers should explore ways to adopt them.	E ngae n anne, ao iai te boraoi ni iango ae kamanenan taetaen te kombiuta aika mano a kona ni kamaunai aekan nakobuaka aika, ao taan karaoi bwain nanon kombiuta a riai ni kakai aia ang ani kamanenai.	
566	Some examples of modern memory safe languages include C#, Rust, Ruby, Java, Go, and Swift.	Taian katoto tabeua iaon Ana Taetae te Kombiuta ae Mano bon te C#, Rust, Ruby, Java, Go, and Swift.	no capitals
567	Read NSA's memory safety [1}[2}information sheet{3]{4] for more.	Wareka ana beeba NSA kamanoan ururing[1}[2}beban rongorongona{3]{4] ao tabeua riki.	
568	**[1}Secure Hardware Foundation.**{2]	[1}Botaki Ibukin Te Kombiuta ae Mano.{2]	
569	Incorporate architectural features that enable fine- grained memory protection, such as those described by Capability Hardware Enhanced RISC Instructions (CHERI) that can extend conventional hardware Instruction-Set Architectures (ISAs), as well as other features like Trusted Platform Modules and Hardware Security Modules.	Te uaia ni waki ma Bwain nanon Kombiuta aika boou are a na kona ni karaoa tiatianakin mwakurin taetaen te kombiuta ibukin kauarerekean te kanganga , n aron are a oti n te Aron Kakorakoran te Kombiuta n totokoi Tokobito(CHERI) ni kabwabwaka maiun kombiuta Instruction-Set Architectures (ISAs).	
570	For more information visit, University of Cambridge's [1}[2}CHERI webpage{3]{4].	Ibukin rongorongona. Nora, Te Kura ae Rietata i Cambridge[1}[2}CHERI uebutiati[3]{4].	
571	**[1}Secure Software Components (SSDF PW 4.1).**	**[1}Bwain Kombiuta Aika Mano (SSDF PW 4.1).**	
572	{1]Acquire and maintain well-secured software components (e.g., software libraries, modules, middleware, frameworks) from verified commercial, open source, and other third-party developers to ensure robust security in consumer software products.	{1]Karekei ao ni kateimatoai kamanomano ni bwain nanon kombiuta aika mano, (e.g., raiburii karaobwai, mwakorona, bwain nanona, tein mwakuri) man bitiniti ake a tia ni kabwataki, ake akea booia, ao taan buroukuraem ana kakoaua bwa te kamano ni bwain nanon kombiuta a raoiroi kabonganaia ibukia katitamwati.	
573	**[1}Web template frameworks (SSDF PW.5.1).**	**[1}Uebutiati ibukin tein karaobwai (SSDF PW.5.1).**	
574	{1]Use web template frameworks that implement automatic escaping of user input to avoid web attacks such as cross-site scripting.	{1]Kabonganai uebutiati ibukin tein karaobwai aika kona ni karaoi kamaunaan mwin ana taibi te tia kabongana ae maiu bon irouna n totokoi tokobito man uebutiati. .	
575	**[1}Parameterized queries (SSDF PW 5.1).**	**[1}Titiraki aika Uatao (SSDF PW 5.1).**	
576	{1]Use parameterized queries rather than including user input in queries, to avoid SQL injection attacks.	{1]Kamanena titiraki aika Uatao nakon ae kona n rekereke, ma katokan te tokobito nakon kanoan te Kombiuta ae te SQL.	
577	**[1}Static and dynamic application security testing (SAST/DAST)**{2] (SSDF PW.7.2, PW.8.2).	**[1}Tuoan manon te karaobwai ae aki bibitaki ao ae bibitki**	

		(SAST/DAST){2] (SSDF PW.7.2, PW.8.2):	
578	Use these tools to analyze product source code and application behavior to detect error-prone practices.	Kamanenai bwain mwakuri n neneri aron karaoan bwai irouia taan karaobwai ao katein karaobwai ibukin kinakin waaki aika-kakarika te kanganga.	
579	These tools cover issues ranging from improper management of memory to error prone database query construction (e.g., unescaped user input leading to SQL injection).	Ma mwakuri ibukin barongaan titiraki ibukin kombiuta aika kai rootaki. (katoto., aki katokan te karinrin man tabo tabeua e na kairiki man te tokobito ae te SQL).	ena kai riki
580	SAST and DAST tools can be incorporated into development processes and run automatically as part of software development.	N aron te SAST ao te DAST a kona ni kabonganaki n tain te karaobwai ao ni maeu iboni irouna bwa katamaroa nakon bwain nanon kombiuta.	add
581	SAST and DAST should complement other types of testing, such as unit testing and integration testing, to ensure products comply with expected security requirements.	Te SAST ao te DAST a irekereke ni waki ma bwai n tutuo ake tabeua, n aron tuoan te karaobwai ao tuoan aron te katomatoma, ni kakoaua bwa te karaobwai e iri nanon kainibaire ibukin kamanomano ake a kantaningaki.	
582	When issues are identified, manufacturers should perform root-cause analysis to systemically address vulnerabilities.	Ngkana iai kanganga, taan karaobwai a riai n neneri nako boton te kangagna ni kakaei memere ke kabwaka n te tititem.	
583	**[1}Code review**{2] (SSDF PW.7.1, PW.7.2).	**{1]Tuoan ana Taetae te Karaobwai**{2] (SSDF PW.7.1, PW.7.2).	
584	Strive to ensure that code submitted into products goes through quality control techniques such as peer review by other developers or "error seeding."	Kabanea nanom ni kakoaua bwa te naan taetae ake a uotakirake ana rinanoaki irouia tabeman taan buroukuraem ibukin uarokoana nakon ae "tamaroa-riki."	
585	[1}[2}Software Bill of Materials (SBOM){3]{4][5} {4](SSDF PS.3.2, PW.4.1).	[1}[2}Aron Tein Karaoan Bwain nanon Kombiuta(SBOM){3]{4][5} {4] (SSDF PS.3.2, PW.4.1).	
586	Incorporate the creation of SBOM[1}4{2][3} [4]{2]to provide visibility into the set of software that goes into products.	Ni kaiireiti kario n te SBOM[1}4{2][3} [4]{2]ni katauraoi kataratara ibukin bwain nanon kombiuta ake ana rin bwa kanoan te karaobwai.	kai n reiti
587	**[1}Vulnerability disclosure programs** {2](SSDF RV.1.3).	**[1}Burokuraem ibukin kaotan kabwaka** {2](SSDF RV.1.3).	
588	Establish vulnerability disclosure programs that allow security researchers to report vulnerabilities and receive legal safe harbor in doing so.	Kawenei aron karaoan Burokuraem Ibukin Kabwakan te intanete are e na anganiia taan kamatebwaia aron te kamanomano bwa ana kona n ribotini kabwaka ao ni mano iaan te tua inanon aia tai ni mwakuri.	
589	As part of this, suppliers should establish processes to determine root causes of discovered vulnerabilities.	Itoman ma, taan karao bwain nanon kombiuta ni kakai anga ake a kona n reke boton te kanganga ma taian kabwaka.	
590	Such processes should include determining whether adopting any of the secure by design practices in this document (or other similar practices) would have prevented the introduction of the vulnerability.	Aia anga ni kakai aikai ana riai ni kona ni kunea ngkana kamanenan te waaki iaon Kamanomano Man Karaoana aika a maroroakinaki ikai, a kona ke aki kona n totokoa te reken te kanganga ngke arona bwa a kabonganaki.	
591	**[1}CVE completeness.**	**[1}Barongaan te CVE.**	

592	{1]Ensure that published CVEs include root cause or common weakness enumeration (CWE) to enable industry-wide analysis of software security design flaws.	{1]E na kakoauaaki bwa memere ni bwain kombiuta (CVE) ake a koreaki e airi ma aron reken te kanganga ao ni ikotaki ma kanganga ake a bon tabangaki (CWE) e aonga ni kona ni bane te koraki ni kakaea-boton raoi te kanganga.	
593	While ensuring that every CVE is correct and complete can take extra time, it allows disparate entities to spot industry trends that benefit all manufacturers and customers.	Ao n kaotia bwa taian CVE ana riai n eti ao taobaraki, iran nanon aio ao ana kona botaki aika kakaokoro n noori anga aika kona iai ni mabiao iai taan bobwai ao karaobwai.	
594	For more information on managing vulnerabilities, see CISA's [1}[2}Stakeholder-Specific Vulnerability Categorization (SSVC) guidance.{3]{4]	Ibukin riki rongorongo iaon barongan memere, noora CISA [1}[2} Bonoti-Utun Memere ae Onoti-nakoia taan bwaibwai (SSVC) te Kairi.{3]{4]	k
595	**[1}Defense-in-Depth.**{2]	**[1}Katamaroan-Totokoan-Kanganga.**{2]	
596	Design infrastructure so that the compromise of a single security control does not result in compromise of the entire system.	Karaoi bwai n teia are ngkana e rotaki te itera teuana ao e na aki roota te tititem.	
597	For example, ensuring that user privileges are narrowly provisioned, and access control lists are employed can reduce the impact of a compromised account.	N aron te kabotau iai, anganakia taan kamanena te intanete te kariaia ae uarereke ao n tiatianaki ao aroia ni kabongana te intanete e na taraki raoi, aio e kona ni kauarerekei mwakuri buaka man taian akaunti n tokobito.	
598	Also, software sandboxing techniques can quarantine a vulnerability to limit compromise of an entire application.	Ao,anganiia taan kamanena te akaunti ni kakatai e kona ni kauarerekea rotakin bwain nanon te kombiuta.	add
599	**[1}Satisfy Cybersecurity Performance Goals (CPGs).**{2]	**[1}Kouru ibukin Kakoroan Nanon te Kamanomano n te Intanete (CPGs).**{2]	
600	Design products that meet basic security practices.	Karaoakin bwain nanon te Kombiuta ao kombiuta aika a ira nanon tein te karaobwai.	k
601	CISA's [1}[2}Cybersecurity Performance Goals{3]{4] outline fundamental, baseline cybersecurity measures organizations should implement.	CISA[1}[2}Ana Kouru ibukin Kakoroan Nanon te Kamanomano n te Intanete{3]{4] e kawenei kakawakin karaobwai bwa ana ira tein te karaobwai ae na bwainaki n taian rabwata nako.	
602	Additionally, for more ways to strengthen your organization's posture, see the UK's [1}[2}Cyber Assessment Framework{3]{4] which shares similarities to CISA's CPGs.	Ao, ibukin riki kakorakoran taran taian rabwata ake ko kona n noora [1}[2}Aron Tuoan te Intanete{3]{4] n te UK Are e kuri n titabo ma ana CPG te rabwata ae CISA.	
603	If a manufacturer fails to meet the CPGs— such as not requiring phishing-resistant MFA for all employees— then they cannot be seen as delivering secure by design products.	Ngkana e aki kakoroi nanon CPG te tia karaobwai— n aron ae aki kariaia tuoaia aia taan mwakuri ae ana tuoaki ibukin karaoan mwakuri buaka n te intanete— man anne ao a kona n taraaki aia bwai bwa e aki mano karaoaia.	
604	The authoring organizations recognize that these changes are significant shifts in an organization's posture.	Rabwata ibukin boretiakin rongorongo n te intanete e ataia ae bitaki aikai a kakawaki ibukia rabwata nako.	
605	As such, their introduction should be prioritized based on tailored threat	Ao e a riai ngkanne, ni moanibwaiaki bwainakiia ae boboto iaon	

	modeling, criticality, complexity, and business impact.	kainnanoana, kangangana ao aron rotan bitiniti.	
606	These practices can be introduced for new software and incrementally expanded to cover additional use cases and products.	Anga aikai a kona ni bwainaki ibukin Bwain Kombiuta aika boou ao man karababaki kabonganakia nakon aron kamanenakia ao karaobwai.	bwain kombiuta
607	In some cases, the criticality and risk posture of a certain product may merit an accelerated schedule to adopt these practices.	N tabetai ao aron kainanoan kainibaire aikai iaon karaobwai tabeua ao e a kona n riai ngkanne n te tai ae waekoa.	
608	In others, practices can be introduced into a legacy codebase and remediated over time.	N tabetai, ao kainibaire aikai a kona ni karinaki inanon tein te karaobwai ao n tutuoaki ni katoa tai.	
609	4[1} [2]Some of the authoring organizations are exploring alternate approaches to gaining security assurances around the software supply chain.{3]	4[1} [2]Tabeman taan anga kariaia a neweabai anga tabeua ao kawai ibukin karekean kamano ni irekereke ma ana taan katauraoi karaobwai.{3]	
610	**SECURE BY DEFAULT TACTICS**	**ARON TE KAMANO MAN TEINA**	
611	In addition to adopting secure by design development practices, the authoring organizations recommend software manufacturers prioritize secure by default configurations in their products.	I rarikin bwainakin Kamanomano-man-teina, taian rabwata ibukin boretiakin rongorongo n te intanete a ibuobuoki nakoia taan karaoa Bwain Nanon te Kombiuta bwa ana moanibwaia aron te Kamanomano-man-Teina.	kamano man teina
612	These should strive to update products to conform to these practices as they are refreshed.	Ao man iri nanon kaetieti aikai engae ngkana iai te bitaki.	
613	For example:	Te kabotau:	
614	**•[1][2}Eliminate default passwords.**{3]	**•[1][2}Kakean Irin Taeka aika Raba.**{3]	no capitals
615	Products should not come with default passwords that are universally shared.	Karaobwai ana riai aia Taeka Aika Raba n aki Iri ke ni kona n tabangaki kabonganana.	no capitals
616	To eliminate default passwords, the authoring organizations recommend products require administrators to set a strong password during installation and configuration or for the product to ship with a unique, strong password for each device.	Ibukin kakean Irin Taeka aika Raba, ao rabwata ibukin boretiakin rongorongo n te intanete e anganiia tabeia taan tararuai karaobwai ae ana riai ni matoatoa taeka aika raba ake karinani bwain nanon kombiuta.	
617	**•[1][2}Mandate multifactor authentication ({**3][4}[5}MFA**{6]{3][2}) for privileged users.**	**•[1][2}Kamatoa te kinaki ae matoa(**{3][4}[5}MFA**{6]{3][2}) ibukia taan kabongana te karaobwai.**	
618	{1]We observe that many enterprise deployments are managed by administrators who have not protected their accounts with MFA.	{1]Ti nonoria ao kambwana tabeua a kabutaki irouia taan tararua aika aki kabongana aron te kinaki ae matoa ae te MFA.	
619	Given that administrators are high value targets, products should make MFA opt-out rather than opt-in.	Ibukina bwa taan tararua ngaia aika ana taketenaki moa irouia tan tokobito, karaobwai a riai ni karaoa te MFA ibukin te-otinako ao tiaki ibukin te-rinnako.	
620	Further, the system should regularly prompt the administrator to enroll in MFA until they have successfully enabled it on their account.	Ao riki te tititem e riai ni kaokioka ana kauring nakoia taan tararua te	

		tititem bwa ana kamaua te MFA n aia akaunti	
621	Netherlands' NCSC has guidance that parallels CISA's, visit their [1}[2}Mature Authentication Factsheet{3]{4] for more information.	Ana NCSC te Netherlands' iai ana kainibaire ae titebo teina ma ana kainibaire CISA, kawara aia Boki ae [1}[2}Koaua ibukin Kinakim{3]{4] ibukin rogorongona ae bwanin.	
622	**•[1][2}Single sign-on (SSO).**	**•[1][2}Katauan teuana Rinim (SSO).**	r
623	{1]IT applications should implement single sign on support via modern open standards.	{1]Bwain nanon te Kombiuta a riai ni Kataua Teuana Rinim n aia rabakau ae boou, n ira nanon kainibaire aika boou.	
624	Examples include Security Assertion Markup Language (SAML) or OpenID Connect (OIDC.)	Katoto tabeua Anganakin te kambwana are e katomako ma te intanete Taekam Nako (SAML) ke Kaotan Taekam nako Nakoia Manatia n te Karaobwai (OIDC.) Aio e riai n aki kaboaki.	
625	This capability should be made available by default at no additional cost.	Te konabwai aio e riai ni katauraoaki n tein te karaobwai n akea boona.	
626	**•[1][2}Secure Logging.**	**•[1][2}Rinim ae Mano.**	
627	{1]Provide high-quality audit logs to customers at no extra charge or additional configuration.	{1]Kataoraoi mwiin rinin ao otinakoia katitamwa aika-tikiraoi n akea boona ke manga kumetoana.	
628	Audit logs are crucial for detecting and escalating potential security incidents.	Tauan mwiin aikai a kakawaki ibukin atakin mwakuri n tokobito ao kakaeaia taan tokobito.	
629	They are also crucial during an investigation of a suspected or confirmed security incident.	A rangi ni kakawaki riki n tain kakaean kanganga nte kamano akea a ataaki ao ake a kantaningaki.	ake a
630	Consider best practices such as providing easy integration with security information and event management (SIEM) systems with application programming interface (API) access that uses coordinated universal time (UTC), standard time zone formatting, and robust documentation techniques.	E riai kamanenaan anga n totoko aika tamaroa n aron katoman taian karaobwai ma rongorongon te kamanomano ao tararuan te Mwakuri n tain te rinnako ae (SIEM) bwai ni katomatoma (API) ena kabonganaaki ibukin rinim ao otinakom, ao ena titabo ma aron kaetan te tai (UTC).	m
631	**•[1][2}Software Authorization Profile.**	**•[1][2}Taekam Nako ibukin Kabwatam n rin n te Karaobwai.**	
632	{1]Software suppliers should provide recommendations on authorized profile roles and their designated use case.	{1]Taan karaobwai a riai ni katauraoi taeka ni ibuobuoki iaon aron kabwatan taekam ibukin mwakuriam arom ni kabongana te karaobwai.	
633	Manufacturers should include a visible warning that notifies customers of an increased risk if they deviate from the recommended profile authorization.	Taan karao bwai ana riai ni karaoa te kamatata ae koona n nooraki iaon aia karaobwai ae kaotia nakon te katitamwa bwa ana iai te kanganga ngkana aki ira aron karaoan Taekaia nako.	
634	For example, medical doctors can view all patient records, but a medical scheduler has limited access to certain information that is required for scheduling appointments.	Te katoto, taokita ana kona n noori rongorongon aia aoraki, ma te tia mwakuri e na aki noori rongorongoia aoraki. Ma e na ti kona n noori	

		araia ma aia tabo ao ana tai te aoraki ma te taokita.	
635	•**[1][2}Forward-looking security over backwards compatibility.**{3]	•**[1][2}Nooran-Kanganga man Taraan Mwakurina aika amaan.**{3]	no capitals
636	Too often, backwards- compatible legacy features are included, and often enabled, in products despite causing risks to product security.	Angin te tai ao Taraan Mwakurin karaobwai ake ngkoa bon iai naba inanon karaobwai, ao a kamaiuaki inanon karaobwai e ngae ngke a kona ni karika te kanganga.	no capitals
637	Prioritize security over backwards compatibility, empowering security teams to remove insecure features even if it means causing breaking changes.	Moani bwaia Taraan Mwakurin Karaobwai aika a maan, ao kariaia taan mwakuri bwa ana kona ni kanakoi teia ake ngkoa ake aki mano e aoria ngkana e na iai te bitaki nakon te karaobwai.	
638	• **[1}Track and reduce "hardening guide" size.**{2]	• **[1}Anoai ao Kauarerekei buburan "Kaetieti ni Kamatoa".{2]**	
639	Reduce the size of "hardening guides" that are included with products and strive to ensure that the size shrinks over time as new versions of the software are released.	Kauarerekei buburan "Kaetieti ni Katamaroa" ake a karaoaki ibukin karaobwai ao keiaki ni koaua bwa e na uarereke ngkana a manga otinako katamaroa aika boou iaon te karaobwai.	
640	Integrate components of the "hardening guide" as the default configuration of the product.	Ikoti "Kaetieti ni katamaroa" bwa e na riki bwa aron kabonganan te karaobwai ni moan teina.	
641	The authoring organizations	Te rabwata ibukin boretiakin rongorongo n te intanete	
642	CISA | NSA | FBI | ACSC | CCCS | CERT NZ | NCSC-NZ | NCSC-UK | BSI | NCSC-NL	CISA | NSA | FBI | ACSC | CCCS | CERT NZ | NCSC-NZ | NCSC-UK | BSI | NCSC-NL	
643	NCSC-NO | NÚKIB | INCD | KISA | NISC-JP | JPCERT/CC | CSA | CSIRTAmericas	NCSC-NO | NÚKIB | INCD | KISA | NISC-JP | JPCERT/CC | CSA | CSIRTAmericas	
644	**TLP:CLEAR**	**TLP:CLEAR**	
645	**TLP:CLEAR**	**TLP:CLEAR**	
646	[1]	[1]	
647	recognize that shortened hardening guides result from ongoing partnership with existing customers and include efforts by many product teams, including user experience (UX).	e kina ae kauarerekean kaetieti ni katamaroa e na reke tii man aia namakin ni katamaroa katitamwa, taan karaobwai(UX).	
648	**•[1]Consider the user experience consequences of security settings.**	**•[1]Taraia raoi bwa te katitamwa e na aki rotaki man waki ni Kamanomano.**	
649	[1}Each new setting increases the cognitive burden on end users and should be assessed in conjunction with the business benefit it derives.	[1}Ni katoa tai are e rin te katamaroa n te karaobwai, ao e rota aron kabonganana a riai n taraki katitamwa ao ni kaieieaki ma mabiaon te kambwana iai.	
650	Ideally, a setting should not exist; instead, the most secure setting should be integrated into the product by default.	Ni bon arona, e riai n aki akea tein te karaobwai, e riai ni kaman rin te Kamano nte moan tai.	
651	When configuration is necessary, the default option should be broadly	Ngkana iai te bitaki ae riai, teina are ma ngkoa e riai ni mano man	

	secure against common threats.{1]	kakamaku aika a okioki.{1]	
652	The authoring organizations acknowledge these changes may have operational effects on how the software is employed.	Te rabwata ibukin boretiakin rongorongo n te intanete a kariaia ae bitaki aikai a kona n rota aron mwakurin ao kabonganan karaobwai.	
653	Thus, customer input is critical in balancing operational and security considerations.	Ngaia are, e kakawaki aia iango katitamwati bwa e na kabaeranta aron kabonganana ao kamanoan karaobwai.	
654	We believe that developing written roadmaps and executive support that prioritize these ideas into an organization's most critical products is the first step to shifting towards secure software development practices.	Te rabwata ibukin boretiakin rongorongo n te intanete a kakoaua ae ngkana taian kawai ao nake ieta nakoaia a boutokai iango aikai ni kabonganai nakon aia karaobwai ao aio ngkanne e na noraki bwa te moan mwaneka ibukin karaobwai aika mano.	
655	While customer input is important, we have observed important cases where customers have been unwilling or unable to adopt improved standards, often network protocols.	E kakawaki aia iango katitamwati, Te rabwata ibukin boretiakin rongorongo n te intanete e a tia n nonoria ae n tabetai katitamwati a rawa ni iraa te bitaki ae boou ibukin te kamanomano.	t
656	It is important for the manufacturers to create meaningful incentives for customers to stay current and not allow them to remain vulnerable indefinitely.	E kakawaki irouia taan karaobwai bwa ana karaoi anainano nakoia katitamwati e aonga n anaaki nanoia ni iriri taian bitaki.	
657	CISA | NSA | FBI | ACSC | CCCS | CERT NZ | NCSC-NZ | NCSC-UK | BSI | NCSC-NL	CISA | NSA | FBI | ACSC | CCCS | CERT NZ | NCSC-NZ | NCSC-UK | BSI | NCSC-NL	
658	NCSC-NO | NÚKIB | INCD | KISA | NISC-JP | JPCERT/CC | CSA | CSIRTAmericas	NCSC-NO | NÚKIB | INCD | KISA | NISC-JP | JPCERT/CC | CSA | CSIRTAmericas	
659	**TLP:CLEAR**	**TLP:CLEAR**	
660	**TLP:CLEAR**	**TLP:CLEAR**	
661	[1]	[1]	
662	**HARDENING VS LOOSENING GUIDES**	**KAMATOAN VS KAMARAUAN KAETIETI**	
663	Hardening guides may result from the lack of product security controls being embedded into a product's architecture from the start of development.	Kaetieti ibukin kamatoan karaobwai e kona n reke man aki taun manon te karaobwai ake a karinaki nte karaobwai mai moan karaoana.	
664	Consequently, hardening guides can also be a roadmap for adversaries to pinpoint and exploit insecure features.	Ao n tokina, ao kamatoan kaetieti e a kona n reke bwa kanga ai te kawai ibukin kaotan aki manon raoi te karaobwai.	
665	It is common for many organizations to be unaware of hardening guides, thus they leave their device configuration settings in an insecure posture.	E tiraua rabwata aki atai aron kamatoan kaetieti, ngaia are a katikui aia karaobwai n teina ae aki mano.	
666	An inverted model known as a loosening guide should replace such hardening guides and explain which changes users should make while also listing the resulting security risks.	Kaitaran aio e ataki n arana ae Kamarauan Kaetieti ae e riai n onei mwin taian kaetieti ake a matoa ao man kabwarabwarai bwa enga bitaki ae ana iria katitamwati ao ni kaoti naba rinanin nako kanganga ake a kona n riki man aio.	no capitals
667	These guides should be written by security practitioners who can explain the tradeoffs in clear language to increase the chances of them being applied correctly.	Irarikin karaoan kaetieti aika matoa ae e airi ma anga ibukin kamanoan te karaobwai.	
668	Rather than developing hardening guides that list methods for securing products, the authoring organizations recommend software manufacturers	Te rabwata ibukin boretiakin rongorongo n te intanete e taeka ni bau nakoia taan karaobwai bwa ana ira tein karaobwai ae mano man teina	

	shift to a secure by default approach and providing "loosening guides."	ao a “kamaraui aia kaetieti.”	ni
669	These guides explain the business risk of decisions in plain, understandable language, and can raise organizational awareness of risks to malicious cyber intrusions.	Kaetieti aikai a kabwarabwarai kanganga aika kona n riki n te aro ae matata iaon beeba, ao e kanongoraa. ao taan karaobwai a kona ni kakorakora aia mwatai iaon totokoan kanganga aika rereke man te tokobito iaon te intanete.	delete
670	Security tradeoffs should be determined by the customers’ senior executives, balancing security with other business requirements.	Taian ananga ni kabuanibwai ana riai n taraki raoi irouia ake a tabe ma aroia katitamwati, ao ni kabaeranta aron te kamano irian ana waki nako te kambwana.	
671	CISA | NSA | FBI | ACSC | CCCS | CERT NZ | NCSC-NZ | NCSC-UK | BSI | NCSC-NL	CISA | NSA | FBI | ACSC | CCCS | CERT NZ | NCSC-NZ | NCSC-UK | BSI | NCSC-NL	
672	NCSC-NO | NÚKIB | INCD | KISA | NISC-JP | JPCERT/CC | CSA | CSIRTAmericas	NCSC-NO | NÚKIB | INCD | KISA | NISC-JP | JPCERT/CC | CSA | CSIRTAmericas	
673	**TLP:CLEAR**	**TLP:CLEAR**	
674	**TLP:CLEAR**	**TLP:CLEAR**	
675	[1]	[1]	
676	**RECOMMENDATIONS FOR CUSTOMERS**	**TAEKA NI BAU NAKOIA KATITAMWA**	
677	The authoring organizations recommend organizations hold their supplying software manufacturers accountable for the security outcomes of their products.	N ana taeka ni bau te rabwata ibukin boretiakin rongorongo n intanete bwa ana bukintaeka taan karaobwai ngkana iai kanganga man aia karaobwai.	
678	As part of this, the authoring organizations recommend that executives prioritize the importance of purchasing secure by design and secure by default products.	Ao e katurua naba nakoia rabwata nako kakawakin kaboan karaobwai aika Mano man Karaoaia ao Teia.	no capital letters
679	This can manifest through establishing policies requiring that IT departments assess the security of software before it is purchased, as well as empowering IT departments to push back if necessary.	E kona n oti aio man kainibaire ibukia kaain te tabo n IT bwa ana tuoi manon karaobwai imwain kaboaia, ao ni kainaomataia bwa ana totoko ngkana e riai.	
680	IT departments should be empowered to develop purchasing criteria that emphasize the importance of secure by design and secure by default practices (both those outlined in this document and others developed by the organization).	Ana kona naba ni karaoi tuan te bobwai aika kaineti ma te Kamano man Karaoana ao Teina (a koreaki aikai nte beeba aio ao tabeua a karaoaki man rabwata tabeua).	k
681	Furthermore, IT departments should be supported by executive management when enforcing these criteria in purchasing decisions.	N reitaki ma ann, ao kaain te tabo n IT a riai ni boutokaki irouia aia mataniwi ngkana a karaoi kaeti ibukin karaoan iango imwain te bobwai.	anne
682	Organizational decisions to accept the risks associated with specific technology products should be formally documented, approved by a senior business executive, and regularly presented to the board of directors.	Mataniwi ana boutoka ni kakoroi nanon tua ake a karaoi. Man taui mwin karaobwai aika aki mano ao ni kakaotaki ni katoa Bowin te Baba n Tararua.	no capital letters
683	Key enterprise IT services that support the organization’s security posture, such as the enterprise network, enterprise identity and access management, and security operations and response capabilities, should be seen as critical business functions that are funded to align with their	Kaain te tabo n IT n te Kambwana ake a boutoka tamaroan manon te kambwana, n aron ana tititem te kambwana, barongaan te rinnako ao atakin ae rinnako, a riai n taraaki bwa ana waaki te kambwana aika moanbaan te kakawaki, ana mwanenaki ni kaitara ana kouru te	k

	importance to the organization's mission success.	kambwana.	
684	Organizations should develop a plan to upgrade these capabilities to leverage manufacturers that embrace secure by design and secure by default practices.	Ana karaoa te katauraoi ibukin katamaroa nakon taobaran kanganga ao ni kabonganai karaobwai ake a iri kaetieti ibukin kamano man karaoana ao Teina.	t
685	Where possible, organizations should strive to forge strategic relationships with their key IT suppliers.	Ngkana e kona, aoi kambwana ma tan karaobwai a riai ni karaoi reitaki ma taan karekeia aia IT.	ao
686	Such relationships include trust at multiple levels of the organization and provide vehicles to resolve issues and identify shared priorities.	Reitaki aikai a riai n reke iai te onimakinaki ni mwangan nako te kambwana ao ni katauraoi anga ni bwainaoraki kanganga ao ni kotei bwai ake a moanibwai.	
687	Security should be a critical element of such relationships and organizations should strive to reinforce the importance of secure by design and secure by default practices in both the formal (e.g., contracts or vendor agreements) and informal dimensions of the relationship.	Te kamano e riai n riki bwa boton te reitaki ao kambwana aikai a riai ni keiaki ni kamatoai aron bonganan te Kamanomano manKaraoana ao n Teina n te boraraoi raoi (e.g.,te boraraoi ma taan kabonako bwai) ao ai boraraoi i nanoa ibukin te reitaki ae tamaroa.	
688	Organizations should expect transparency from their technology suppliers about their internal control posture as well as their roadmap towards adopting secure by design and secure by default practices.	A riai n kataua naba taan karaobwai bwa e na kirati aron tauan mwiin aron aia bwai taan kabonakoi bwaai ao ni matata naba bwa tera ae ana riai ni kakaraoia ibukin te Kamano man Karaoana ao Teina.	
689	CISA | NSA | FBI | ACSC | CCCS | CERT NZ | NCSC-NZ | NCSC-UK | BSI | NCSC-NL	CISA | NSA | FBI | ACSC | CCCS | CERT NZ | NCSC-NZ | NCSC-UK | BSI | NCSC-NL	
690	NCSC-NO | NÚKIB | INCD | KISA | NISC-JP | JPCERT/CC | CSA | CSIRTAmericas	NCSC-NO | NÚKIB | INCD | KISA | NISC-JP | JPCERT/CC | CSA | CSIRTAmericas	
691	**TLP:CLEAR**	**TLP:CLEAR**	
692	**TLP:CLEAR**	**TLP:CLEAR**	
693	[1]	[1]	
694	In addition to making secure by default a priority within an organization, IT leaders should collaborate with their industry peers to understand which products and services best embody these design principles.	Ni ikotaki ma karaoan kamano man teina te moanibwai irouia taan karaobwai, taan kairiri nte IT ana karekebai ba raoia ni mwakuri n aia kambwana ibukin kakaea aron barongaan kaetieti ibukin karaoan aia karaobwai ao tieweti.	
695	These leaders should coordinate their requests to help manufacturers prioritize their upcoming security initiatives.	Taan kairiri aikai a riai ni barongai aron aia karekebai ibukin buokan aia kambwana n ata ae moanibwai riki n aia kamano ake a babarongai.	
696	By working together, customers can help provide meaningful input to manufacturers and create incentives for them to prioritize security.	Man te irekenibai ni mwakuri aei, ao katitamwa ana kona ni karini aia iango nakoia kambwana ni karaobwai ao ni karika te unga ibukin karaoan karaobwai ni kamano.	
697	When leveraging cloud systems, organizations should ensure they understand the shared responsibility model with their technology supplier.	Ngkana kambwana ni karaobwai a kabonganai oin aia tiewa, taan kabongai a riai n atai raoi tabeia ma kambwana ni karaobwai.	
698	That is, organizations should have clarity on the supplier's security responsibilities rather than just the customer's responsibilities.	Are nanona bwa, taan kabonganai karaobwai a riai ni matata ae tabeia kaotaia taan kabongana, ao tiaki ti tabeia taan kabongana.	
699	Organizations should prioritize cloud providers that are transparent about their security posture, internal controls, and ability to live up to their obligations under the shared responsibility model.	Taan kabonganai karaobwai a riai ni moanibwaia taan katauraoi tiewa ake a kirati aia waaki n aron kabonganan aia kamano, ao a kakaonimaki ni karaoi tabeia ibukin kabonganan aia tiewa.	
700	DISCLAIMER	TE OTANGA	

701	The information in this report is being provided "as is" for informational purposes only.	Rongorongo aika oti n te riboti aei a katauraoaki "n aroia aei" ti ibukin am rongorongo.	
702	CISA and the authoring organizations do not endorse any commercial product or service, including any subjects of analysis.	CISA, ao taian rabwata ibukin boretiakin rongorongo n te intanete aki inanonano ke ni boutokai aroia taian kambwana ake irekereke ma karaobwai ao korokoan te intanete ni ikotaki ma baike a kabaranakoaki.	
703	Any reference to specific commercial entities or commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise does not constitute or imply endorsement, recommendation, or favoritism by CISA and the authoring organizations.	Atongan taian rabwata ke bwai ni karikirake, aron karaoan bwai, ke taan karaoi nanon bwai, aran kambwana, taan karaobwai ao tabeua riki, tiaki nanona bwa tia katanoatai, ke ni katerei, ke tao a tangiraki iroun CISA ma taian rabwata ibukin boretiakin rongorongo n te intanete.	
704	This document is a joint initiative by CISA that does not automatically serve as a regulatory document.	E karioaki te beba iroun CISA ma raona tabeman ao e aki riki bwa te mwakoro n tua ae ana riai ni iraki nanona.	
705	CISA | NSA | FBI | ACSC | CCCS | CERT NZ | NCSC-NZ | NCSC-UK | BSI | NCSC-NL	CISA | NSA | FBI | ACSC | CCCS | CERT NZ | NCSC-NZ | NCSC-UK | BSI | NCSC-NL	
706	NCSC-NO | NÚKIB | INCD | KISA | NISC-JP | JPCERT/CC | CSA | CSIRTAmericas	NCSC-NO | NÚKIB | INCD | KISA | NISC-JP | JPCERT/CC | CSA | CSIRTAmericas	
707	**TLP:CLEAR**	**TLP:CLEAR**	
708	**TLP:CLEAR**	**TLP:CLEAR**	
709	[1]	[1]	
710	CISA	CISA	
711	[1}[2}CISA's SBOM Guidance{3][4}	[1}[2}Ana Korani kaeti CISA ae te SBOM{3][4}	
712	{1]{2][3}CISA's Cross-Sector Cybersecurity Performance Goals{2]	{1]{2][3}CISA Kouru iaon Makurian Kamanomano n te Intanete N tabo ni mwakuri aika okoro{2]	
713	[1}Guidelines on Technology Interoperability{2]	[1}Kairi iaon kabonganan rabakau aika boou{2]	
714	[1}[2}CISA and NIST's Defending Against Software Supply Chain Attacks{3][4}	[1}[2}CISA ao NIST Aia anga n Totoko nakon Tokobito nakoia Taan karaobwai{3][4}	
715	{1]{2][3}The Cost of Unsafe Technology and What We Can Do About It | CISA{2]	{1]{2][3} Boon Aki Manon Rabakau aika Boou ao arora n Taobarai | CISA {2]	
716	[1}Stop Passing the Buck on Cybersecurity:	[1}Katoki aron memere iaon te intanete:	
717	Why Companies Must Build Safety Into Tech Products (foreignaffairs.com){1]	Bukin tera kambwana a riai ni Karini Kamanomano nakon aia Karaobwai (foreignaffairs.com){1]	
718	[1}CISA's Stakeholder-Specific Vulnerability Categorization (SSVC) Guidance{2]	[1}CISA Bonoti-Utun Memere ae Onoti-nakoia taan bwaibwai (SSVC)Te Kairi{2]	
719	[1}CISA's Phishing Resistant MFA Fact Sheets{2]	[1}CISA Totokoan tokobito MFA Beban koaua tabeua{2]	
720	[1}Cyber Guidance for Small Businesses | CISA{2]	[1}Kairi iaon Intanete ibukia bitiniti aika Uarereke | CISA{2]	
721	NSA	NSA	
722	[1}NSA's Cybersecurity Information Sheet on Memory Safety{2]	[1}NSA Rongorongon aron kamanoan kombiuta iaon te intanete{2]	
723	[1}NSA's ESF Securing the Software Supply Chain:	[1}NSA ESF Kamanoaia taan karaobwai:	
724	Best Practices for Suppliers{1]	Aroaro aika mano ibukia taan karaobwai.{1]	
725	FBI	FBI	
726	[1}Understanding and Responding to the SolarWinds Supply Chain Attack:	[1}Atakin ao aron Kaitaran tokobito aika taan karaoa te buia n ang:	

727	The Federal Perspective{1]	Ana Itera te Tautaeka{1]	
728	[1}The Cyber Threat - Response and Reporting{2]	[1}Kanganga nte Intanete – Kaitarana ao Ribotinakina{2]	
729	[1}FBI's Cyber Strategy{2]	[1}FBI Ana anga iaon te intanete{2]	
730	National Institute of Standards and Technology (NIST)	Botaki n reirei ibukin Waaki aika Tabangaki ao Rabakau aika boou (NIST)	
731	[1}NIST's Digital Identity Guidelines	[1}NIST Te Kairi ibukin Kinakin Kombiuta	
732	{1][2}NIST's Cyber Security Framework	{1][2}NIST Aron Kamanomano iaon te Intanete	
733	{1][2}[3}NIST's Secure Software Development Framework (SSDF){4][5}	{1][2}[3}NIST Aron Karaoan bwain te Intanete ae Mano (SSDF){4][5}	
734	{1]{2]	{1]{2]	
735	Australian Cyber Security Centre (ACSC)	Botaki ni Kamano iaon te intanete I Aotiteria (ACSC)	
736	[1}ACSC's IoT Code of Practice Guidance for Manufacturers	[1}Ana Kaetieti ACSC ibukin aroia Taan Mwakuri ni Karaobwai	
737	{1]	{1]	
738	The United Kingdom's National Cyber Security Centre (UK)	Botaki ni Kamanomano nte Intanete iaon Buritan (UK)	
739	[1}The UK's Cyber Assessment Framework{2]	[1}Kairi ibukin Karaoan ao Kaotinakoan karaowai aika mano man te UK NCSC{2]	
740	[1}The UK NCSC's Secure Development and Deployment guidance{2]	[1}Kairi ibukin Arom n Taobarai memere man te UK NCSC{2]	
741	[1}The UK NCSC's Vulnerability Management guidance{2]	[1}Kairi ibukin Barongan Memere man te UK NCSC{2]	
742	[1}The UK NCSC's Vulnerability Disclosure Toolkit{2]	[1}Bwain Katerean Memere man te UK NCSC{2]	
743	[1}University of Cambridge's CHERI{2]	[1}CHERI Man te Kuura ae Rietata I Cambridge{2]	
744	[1}So long and thanks for all the bits - NCSC.GOV.UK{2][3}[4]{5]	[1}Tiabo ao ko rabwa n am mwakuri - NCSC.GOV.UK{2][3}[4]{5]	
745	Canadian Centre for Cyber Security (CCCS)	Botaki ni Kamanomano iaon te intanete i Kanata (CCCS)	
746	[1}CCCS's Guidance on Protecting Against Software Supply Chain Attacks	[1}CCCS's Kaita iaon Totokoan tokobeto nakoia taan karaobwai	
747	{1][2}Cyber supply chain:	{1][2} Taan Karaobwai n te Intanete:	
748	An approach to assessing risks{1]	Arom ni ukora reken te kanganga{1]	
749	[1}Canadian Centre for Cyber Security's CONTI ransomware guidance{2]	[1}Botaki ni Kamanomano iaon te intanete i Kanata CONTI Kairi ibukin te tautau n te mwane {2]	
750	**Resources**	**Ritioti**	
751	CISA | NSA | FBI | ACSC | CCCS | CERT NZ | NCSC-NZ | NCSC-UK | BSI | NCSC-NL	CISA | NSA | FBI | ACSC | CCCS | CERT NZ | NCSC-NZ | NCSC-UK | BSI | NCSC-NL	
752	NCSC-NO | NÚKIB | INCD | KISA | NISC-JP | JPCERT/CC | CSA | CSIRTAmericas	NCSC-NO | NÚKIB | INCD | KISA | NISC-JP | JPCERT/CC | CSA | CSIRTAmericas	
753	**TLP:CLEAR**	**TLP:CLEAR**	
754	**TLP:CLEAR**	**TLP:CLEAR**	
755	[1]	[1]	
756	Germany's Federal Office for Information Security (BSI)	Botaki man tautaeka n Tiaman ibukin Rongorongo aika Mano (BSI)	
757	[1}The BSI Grundschutz compendium (module CON.8){2]	[1}Te BSI Grundschutz compendium (module CON.8){2]	
758	[1}The international standard IEC 62443, part 4-1{2]	[1}Ae Tieuataake nte Aonnaba IEC 62443, mwakoro 4-1{2]	
759	[1}State of IT-security in Germany report, 2022	[1}Taran Manon-Rabakau iaon te Intanete I Tiaman, 2022	
760	{1][2}BSI practices of web application security{1]	{1][2}BSI aron mwakurian bwain nanon kombiuta aika mano{1]	
761	Netherland's National Cyber Security Centre	Botaki ni Kamano iaon te intanete nte Netherlands	
762	[1}NCSC-NL's Mature Authentication Factsheet{2]	[1}NCSC-NL Boki iaon aron kinankin ae mano riki{2]	
763	Japan's National Center of Incident Readiness and Strategy for	Ana tienta Tiaban ibukin te kakatauraoi ao Anga ibukin te Kamano nte	

	Cybersecurity (NISC)	Intanete (NISC)	
764	[1}Japan’s National Cybersecurity Strategy{2]	[1}Ana anga Tiaban ni kamano man te Intanete{2]	
765	Japan’s Ministry of Economy, Trade and Industry (METI)	Ana Tabo ni Mwakuri Tiaban ibukin Kaubwai, Iokinibwai ao Karikirake (METI)	
766	[1}Guide of Introduction of Software Bill of Materials (SBOM) for Software Management{2]	[1}Kaita ibukin Katerean Tuan bwain nanon kombiuta (SBOM) ibukin Barongan Bwain nanon Kombiuta{2]	
767	[1}Collection of Use Case Examples Regarding Management Methods for Utilizing OSS and Ensuring Its Security{2]	[1}Botan nako mwakuri ao katoto ibukin aron Barongan ao Kabonganan OSS ao Kakoauan ana Kamano{2]	
768	Cyber Security Agency of Singapore	Botaki ni Ibuobuoki ibukin Kamano nte Intanete iaon Singapore	
769	[1}Technical Advisory on Secure API Development{2]	[1}Taeka ni bau ibukin aron karaoan API aika mano{2]	
770	[1}CSA SingCERT Vulnerability Disclosure Policy{2]	[1}CSA SingCERT Kainibaire ibukin Kaotan Memere{2]	
771	[1}CSA SingCERT Incident Response Checklist{2]	[1}CSA SingCERT Aron Tuoan Kaitaran Kanganga{2]	
772	[1}[2}CSA SingCERT Incident Response Playbooks	[1}[2}CSA SingCERT Boki ibukin Kaitaran Kanganga	
773	{1]{2][3}[4}CSA Security by Design Framework{1]{2]	{1]{2][3}[4}CSA Kairi ibukin katean Kamano man Karaoana {1]{2]	
774	[1}CSA Security by Design Framework Checklist{2]	[1}CSA Kairi ibukin tuoan aron katean Kamano man Karaoana{2]	
775	[1}CSA Guide to Cyber Threat Modelling{2]	[1}CSA Kairi ibukin Kinakin tein karaoan Kanganga nte Intanete{2]	
776	[1}CSA Cybersecurity Labelling Scheme{2]	[1}CSA Kario ibukin Tauan mwin Kamano nte Intanete{2]	
777	Other	Tabeua riki	
778	[1}How Complex Systems Fail	[1}Aron Uruakin Tititem aika Bubura	
779	{1][2}The New Look in complex system failure{1]	{1][2}Taratara ae boou n aron uruakin tititem aika bubura{1]	
780	REFERENCES	REBURENTI	
781	\[1] https://csrc.nist.rip/publications/history/ande72.pdf	\[1] https://csrc.nist.rip/publications/history/ande72.pdf	
782	\[2] https://www.cisa.gov/sbom and SBOMs references in TR 03183-2 https://www.bsi.bund.de/dok/TR-03183	\[2] https://www.cisa.gov/sbom ao SBOMs ritioti inanon TR 03183-2 https://www.bsi.bund.de/dok/TR-03183	
783	\[3] Juran on Quality by Design by J.M. Juran, 1992.	Juran ioan Te tamaroa ma Karaoana mairoun J.M.Juran, 1992.	
784	CISA | NSA | FBI | ACSC | CCCS | CERT NZ | NCSC-NZ | NCSC-UK | BSI | NCSC-NL	CISA | NSA | FBI | ACSC | CCCS | CERT NZ | NCSC-NZ | NCSC-UK | BSI | NCSC-NL	
785	NCSC-NO | NÚKIB | INCD | KISA | NISC-JP | JPCERT/CC | CSA | CSIRTAmericas	NCSC-NO | NÚKIB | INCD | KISA | NISC-JP | JPCERT/CC | CSA | CSIRTAmericas	
786	**TLP:CLEAR**	**TLP:CLEAR**	
787	**TLP:CLEAR**	**TLP:CLEAR**	
788	[1]	[1]	