): Jbject: ate: ttachments:	Moody, Dustin (Fed) Kerman, San J. (Fed) RE: Per our discussion Friday, July 29, 2016 5:28:00 AM Iman000.cog			
ne that I hav	ve received!			
	n, Sara J. (Fed) uly 29, 2016 8:27 AM			
	ustin (Fed) <dustin.moody@nist.gov> er our discussion</dustin.moody@nist.gov>			
	the CFP from the lawyers?			
t: Friday, Ju	, Dustin (Fed) uly 29, 2016 8:03 AM			
Regenschei Kerman Sa	eld, Andrew (Fed) < <u>andrew.regenscheid@nist.gov</u> > ara J. (Fed) < <u>sara.kerman@nist.gov</u> >; Chen, Lily (Fed) < <u>lily.chen@nist.gov</u> >	,		
	er our discussion			
I think the	e intent was that the Background section would serve as an intro, but I car we need to add a pointer back to the FRN in our three paragraph RFC as sh		o flip the order of the two. I think we want to make sure people know we want ow?	comments back on this, and so putting the RFC first should help with that.
m: Regense	cheid, Andrew (Fed)			
	y, July 28, 2016 2:25 PM ustin (Fed) < <u>dustin moody@nist.gov</u> >			
Cerman, Sa	ara J. (Fed) < <u>sara kerman@nist.gov</u> > er our discussion			
tin,				
			iments" in the middle- basically it's jammed between the first and second secti lardization? Or was the intent that the Background section of the CFP would se	
	n, Sara J. (Fed)" < <u>sara.kerman@nist.gov</u> > y, July 28, 2016 at 1:14 PM			
Andrew Re	egenscheid < <u>andrew.regenscheid@nist.gov</u> >			
ject: Per ou	Justin (Fed)" < <u>dustin moody@nist.goy</u> > ur discussion			
me know w for Propos	what you and Dustin decide on the location of the RFC link: sals = Section 1 of CFP			
mission Red	eqs = Section 2 of CFP rough Evaluation Process = Section 5 of CFP			
	w Higtory Bookmarks Tools Help			- 6
VIIST.gov - C	Computer Security × 🚾 ServiceNow 🛛 🛛 😽 IRC-Biome	tric Conforman 🗴 🛛 🙆 Multicast Delayed Authenti	. 🗴 🔟 jchalpin   NIST Cyber Com 🗴 📑 DHS Class of 1986 - 25 Year 🗴 🔀	Verizon   My Verizon   Veriz × MM NIST Bibliography Web Ap × +
• 0   file/	:///C:/csrc_working/groups/ST/post-quantum-crypto/rfc-july2016.html		C	🔍 information sciences peralta 🔅 👌 🖄 🦻 🕹
		Post-Quantum Cryptography Project	CSRC HOME > GROUPS > CT > POST-QUANTUM CRYPTOGRAPHY PROJECT	
			CORC HOME > GROOPS > CT > POST-QUANTOM CRTPTOGRAPHT PROJECT	
		Documents	POST-QUANTUM CRYPTO STANDARDIZATION	_
		Documents Workshops / Timeline	POST-QUANTUM CRYPTO STANDARDIZATION Request For Comments On Submission Requirements And	-
		Documents Workshops / Timeline Federal Register Notices Email Listserve	POST-QUANTUM CRYPTO STANDARDIZATION Request For Comments On Submission Requirements And Evaluation Criteria The National Institute of Standards and Technology (NIST) is requesting	-
		Documents Workshops / Timeline Federal Register Motces Email Listserve POC Project Contact	POST-QUANTUM CRYPTO STANDARDIZATION Request For Comments On Submission Requirements And Evaluation Criteria The National Institute of Standards and Technology (NST) is requesting comments on a new process to solicit, evaluate, and standards are or more comments on a new process to solicit, evaluate, and standards are or more comments on a new process to solicit, evaluate on the formation of the solicity of the	
		Documents Workshops / Timeline Federal Register Notices Email Listserve PGC Project Contact Post-Quantum Cryptography	POST-QUANTUM CRYPTO STANDARDIZATION Request For Comments On Submission Requirements And Evaluation Criteria The National Institute of Standards and Technology (NST) is requesting comments on a new process to solid, valuata, and standards one or more apartomic and the process to solid, valuata, and standards one or more apartomic and the process to solid, valuata, and standards one or more apartomic and the process to solid, valuata, and standards one or more apartomic and the process of solid, valuata, and standards one or more apartomic and an origin apartomic apartomic apartomic aparts solid apartomic aparts and the solid aparts of the solid aparts solid aparts and the solid aparts of the solid aparts of the solid solid aparts of the solid aparts of the solid aparts of the solid solid aparts of the solid aparts of the solid aparts of the solid solid aparts of the solid aparts of the solid aparts of the solid solid aparts of the solid aparts of the solid aparts of the solid solid aparts of the solid aparts of the solid aparts of the solid solid aparts of the solid aparts of the solid aparts of the solid aparts of the solid solid aparts of the solid aparts of the solid aparts of the solid aparts of the solid aparts of the solid aparts of the solid aparts of the soli	
		Documents Wortshopy / Timeline Federal Register Notices Email Listerve POC Project Contact Post-Quantum Cryptography Standardization Call to Proposals	POST-QUANTUM CRYPTO STANDARDIZATION Request For Comments On Submission Requirements And Evaluation Criteria The National Institute of Standards and Technology (NST) is reguesting comments on an emprocess to solid, evaluate, and standards on or more quartum resistant public-key cryptographic algorithms. Currently, public-key cryptographic algorithms are specified in PIS 184–1, Olga Signiture Standard, as well as a special publication SP 605-84. Resiston 2, Standard, as well as a special publication SP 605-84. Resiston 2, Cuartific Torchoradory and SP 6005-88 Resiston 1.	-
		Documents Worshopp 21 Timeline Federal Register Notices Email Listerine PCO Previce Consist Post-Quantum Crystography Standardization Call for Proposals 8470 on Submission Regarments and Sectuation Criteria	POST-QUANTUM CRYPTO STANDARDIZATION Request For Comments On Submission Requirements And Evaluation Criteria The Network of Submission Requirements And evaluation Criteria The Network of Submission Recently (NST) is requesting optimation are not process to solid, evaluat, and standards: one s more quantum resistant public-key cytopraphic algorithms. Currently, public-hay Recommendiation are special publications. SP 800-548 Resiston 2, Recommendiation for ParWork Key Edualment Schemen Zising Discrete Logarithm Crystography and SP 800-568 Resiston 1, Recommendiation there: These algorithms are wherefite to states from Contrologiation Weiner: These algorithms are wherefite to states from	-
		Documents Workshop Timiline Federal Register Notices Email Luterie POC Project Contact Poct-Quantum Cryptography Standardization Call for Troposals Bird'on Admission Registerments and Evaluation Contas	POST-QUANTUM CRYPTO STANDARDIZATION Request For Comments On Submission Requirements And Evaluation Criteria The National Institute of Standards and Technology (NST) is requesting comments on a new process to solid. A walk, and standards one or mere orgorographic algorithms are specified in FIPS 184–1. Digat Signature Standard, as well as special photometry SN0-554 Restors 2. Recommendation for Fair/Wark kay Etablishment Schemen Lising Discrete Pair/Wark Kryc Etablishment Schemen Lising Discrete Pair/Wark Kryc Etablishment Schemen Lising Interform Fair/Wark Kryc Kryc Etablishment Schemen Lising Interform Fair/Wark Kryc Kryc Etablishment Schemen Lising Interform Fair/Wark Kryc Kryc Lising Interform Fai	-
		Decuments Veystanborg Timuline Federal Register Notices Email Lutarie POIC Project Contact Para-Counterno Cytogeography Call for Proposala Refi de domesiane Registrements and Evaluation Cettes Budhensian Registrements	POST-QUANTUM CRYPTO STANDARDIZATION Request For Comments On Submission Requirements And Evaluation Criteria The Network of Standards and Technology (NST) is reguesting comments on a new process to solici, valuate, and standardse one or mer quartum resistant public-key cryptographic algorithms. Currently, public-key comporting algorithms are specified in PST 184–1, Oggis Solinitar Recommendation for Pai-Wiles Key Establishment Schemes Using Darteet Logathin Cryptography and SP 8005 Resiston II. Recommendation for Pai-Wiles KeyE-Establishment Schemes Using Insteade Cryptograph Forew(These Schemes Using Insteade Cryptograph)	
		Decuments Vigrataboy Timulino Federal Register Notices Email Lusterie POIC Project Contact Call for Proposala Call for Proposala Boldmission Requirements Indication Cetteria Evaluation Cetteria Evaluation Cetteria Evaluation Cetteria Evaluation Cetteria	POST-QUANTUM CRYPTO STANDARDIZATION Request For Comments On Submission Requirements And Evaluation Criteria The National Institute of Standards and Technology (NST) is reguesting comments on an exproses to solid, valueta, and standards en or more quantum-resistant public-key cryptographic algorithms. Currently, public-key cryptographic algorithms are special public-key cryptographic algorithms. Currently, public-key Comments on an expression solid. The ST Bi-L Juggs Signiture Standard, as well as special public-key cryptographic algorithms. Currently, public-key Comments on an expression solid. Second Standards and Composition of the Standard Standards Standards and Cryptography Newer: Heast algorithms are volumelish to talcola from large-cale quantum completes leve INSTIR SISE Beat on Phat Justices Are algorithm completes leve INSTIR SISE Depart on Phat Justices Park/Weser: Heast algorithms are volumelish to talcola from large-cale quantum completes leve INSTIR SISE Depart on Phat Justices Are algorithm completes leve INSTIR SISE Depart on Phat Justices Are algorithm completes leve INSTIR SISE Depart on Phat Justices Are algorithm completes leve INSTIR SISE Depart on Phat Justices Are algorithm completes leve INSTIR SISE Depart on Phat Justices Are algorithm to specess. Are algorithm completes and the algorithm and specific and the other Are algorithm to specess. Are algorithm and the algorithm and the algorithm and the algorithm in Specess. Are algorithm and the algorithm and the algorithm and the algorithm and the algorithm in Specess. Are algorithm and the algorithm algorithm and the	
		Documents Worshopp / Timeline Federal Register Natices Email Laterio PCO Proyet Contact Post-Quantum Crystography Standardization Call for Proposals RFC on Submission Registrements and Seaturation Criteria Submission Registrements Minimum, Acceptability Registrements Evaluation Criteria	POST-QUANTUM CRYPTO STANDARDIZATION Request For Comments On Submission Requirements And Evaluation Criteria The National Institute of Barden's and Technology (NST) is sequesting comments on a new process to solid. A weak and standards on or more quantum-resistant public-key cryptographic algorithms. Currently, public-key Standard, as well as a special policitation SP 806-64. Resiston 2, Recommendation on Par-Wise Avg Calibahment Schemen Lising Discrete Par-Wisea Key-Establishment Scheme Lising Integer Factorization Cryptograph: Power, these algorithms are wurberable to tacks from Inge-scale quantum comparies (see <u>WSTR 8156 Espect on Past Quantum</u> Cryptograph: Power, these algorithms are wurberable to tacks from Inge-scale quantum comparies (see <u>WSTR 8156 Espect on Past Quantum</u> Par-Wisea Key-Establishment (see the Criteria et al. Criteria) As a for step in this process, NST is publishing dart minimum acceptablishing adjoctable public optice. Comment, it is intended that the new public-key algorithms to solid public comment, it is intended that the new public-key algorithms to solid public comment, it is intended builts to randize algorithms to solid public comment, it is intended builts that the new public-key moders and the solid public comment. This intended builts that the new public-key algorithms to solid public comment, it is intended builts that the new public-key moders algorithms to solid public comment. This intended builts that the new public-key moders algorithms to solid public comment. This intended builts that the new public-key moders algorithms that the new public-key moders and the new public-key moders.	ay
		Decuments Vigrataboy Timulino Federal Register Notices Email Lusterie POIC Project Contact Call for Proposala Call for Proposala Boldmission Requirements Indication Cetteria Evaluation Cetteria Evaluation Cetteria Evaluation Cetteria Evaluation Cetteria	POST-QUANTUM CRYPTO STANDARDIZATION Request For Comments On Submission Requirements And Kolaution Criteria The National Institute of Standards and Technology (NST) is requesting comments on an express to solid, valuat, and standards are or mere another and the special policities of complexity and the special policities of policy of the special policities	dy ing
		Documents Vorschop / Timeline Federal Register Moticas Emul Luterne POC Project Contact Parts-Countember Companying Call for Transassa Call for Transassa Budrassan Requirements Budrassan Requirements Evaluation Criteria Evaluation Criteria Evaluation Criteria Evaluation Criteria Evaluation Criteria	POST-QUANTUM CRYPTO STANDARDIZATION Request For Comments On Submission Requirements And Evaluation Criteria The International Institute of Standards and Technology (1857) is requesting comments on an express to solid, walks, and standards en or mere antimic messistint public key cryptographic algorithms. Currently, public-solid Standard, and walks and Standards and Technology (1857) is requesting comments on an any process to solid. The Standard and the International Institute of Standards and Technology (1857) is requesting commentation for Fair-Wise Kay: Establishment Stohemes Using Biscrete Legatim Cryptography and SP 80054 Revision. The Commendation for Pair-Wises Key: Establishment Schemes Using Biscrete Legatim Cryptography and SP 80054 Revision. The Commendation for Pair-Wises Key: Establishment Schemes Using Biscrete Legatime Cryptography and SP 80054 Revision. The Commendation for Pair-Wises Key: Establishment Schemes Using Biscrete Legatime Cryptography and SP 80054 Revision. The Commendation for Pair-Wise Key: Establishment Schemes Using Biscrete Legatime Cryptography and SP 80054 Revision. The Commendation for Pair-Wise Key: Establishment Schemes Using Biscrete As a first step in this process. NBT Is publiched and minimum acceptability requerements, submission requerements, and evaluation criteria for candidate stepsisting avairation and labor exciting and key-establishment disportant distrume complexes veryoption, and key-establishment disportant disportantion complexes as analable right-Key excryption. The schemest Ib the abort of quarket complexes. The distrument complexes veryoption and key-establishment formation complexes as analables regut-Key and walkable in the ment the formation of the schemest and evaluation complexes as analable right-Key and walkable for Comment in and the schemest and exclusion formation and the based of the Comment in and the schemest and exclusion formation and the based of the Comment in and the schemest and exclusion formation and the based for Comment in and the s	dy ing
		Documents Vorschop / Timeline Federal Register Moticas Emul Luterne POC Project Contact Parts-Countember Companying Call for Transassa Call for Transassa Budrassan Requirements Budrassan Requirements Evaluation Criteria Evaluation Criteria Evaluation Criteria Evaluation Criteria Evaluation Criteria	POST-QUANTUM CRYPTO STANDARDIZATION Request For Comments On Submission Requirements And Kalautan Criteria The Network of Standards and Technology (SIST) is requesting comment on a networks to solid. Networks and standards are on the process to solid. The Network of Standards are on the Standard, as well and solid are on the Standards Standard, as well as special policitoms 580-564 Restor. 2 Recommendation for Pai-Week kay Establishment Schemen Lising Discret Pai-Wies Refore Stabilishment Schemen Lising Discret Dispracting and the Stabilishment Schemen Lising the Stabilishment Charles and Stabilishment Schemen Lising Integra Factorization Pair Vision (Stabilishment Schemen Lising Integra Factorization Dispracting automatication and schemen Lising Integra Factorization Dispracting automatication and schemen Lising Integra Factorization Conference on the Stabilishment Schemen Lising Integra Factorization Dispracting automatication and schemen Lising Integra Factorization Conference on the Stabilishment Schemen Lising Integra Factorization Dispracting automatication and schemen Lising Integra Factorization Conference on the Stabilishment Schemen Lising Integra Factorization Conference on the Stabilishment Schemen Lising Integra Factorization the advect advect anguarkare, paladoking daft minimum scceedablishment Schemen Integration and Stabilish Integra Integra Automatication Stabilishment Schemen Lising Integra Automatication Stabilishment Ander Automatication and available and the schemen Lising Barbaham the advect of guardian complexis. The daft neglements and evaluation Cristina are analable in the mean to the Integra Barbaham Integra Automatication and Stabilishment Technologication Stabilishment and evaluation cristina are analable in the mean to the Integra Barbaham Integra Barbaham Schement and Stabilishment Technologication Stabilishment and evaluation Cristina are analable in the mean to the Integra Barbaham Integra Barbaham Integra Barbaham Integra Barbaham Stabilishment An	dy ing
		Documents Vorschop / Timeline Federal Register Moticas Emul Luterne POC Project Contact Parts-Countember Companying Call for Transassa Call for Transassa Budrassan Requirements Budrassan Requirements Evaluation Criteria Evaluation Criteria Evaluation Criteria Evaluation Criteria Evaluation Criteria	POST-QUANTUM CRYPTO STANDARDIZATION Request For Comments On Submission Requirements And Evaluation Criteria The Network of Standards and Technology (NST) is requesting comments on a reprocess to solic, what, and standards en or more quartum resistant public-key cryptographic algorithms. Currently, public key cryptografic algorithms are specified in TeS 184-1, Quigs Standards Recommendation for Flaw-Wiles Key Establishment Schemes Using Darente Logatimic Cryptograph (Nover) the Schemes Using Darente Cryptograph (Nover) these algorithms are submitted to algorithms Cryptograph (Nover) these algorithms are submitted to algorithms (Nover). Cryptograph (Nover) these algorithms are submitted to algorithms (Nover). As a first for the Process. NST is rended that here public-key cryptograph (Nover), the algorithms is indeed by the new public key cryptograph (Nover). In the index of the Internet of the algorithm Comments, submission requirements, and evaluation citeria for candidation algorithms to submission requirements, and evaluation citeria for candidation table calculated and spacets, NST is the redet of that here public-key cryptograph (Nover). In the interest of the Internet of the table calculated and spacets, NST is and evaluation citeria for candidation assessing operments in devaluation citeria are available in the meut to the table address of quarks and evaluation. Certaria are available in the meut to the table address of quarks and evaluation corteria are available in the remet to the the address of quarks and collable and the meutor to the comment to formation will rise the forse-stable function corterial assessing comment information will rise the forse-stable function corterial comments to <u>goorement redevaluation</u> corteria are available in the remute to the comment to formation and instandation and citeria and calable in the remute to the comment to <u>formation and strables</u> and the corterial to <u>formation and the corterian</u> and the corterian and the corterian and the corteria	dy ing
		Documents Vorschop / Timeline Federal Register Moticas Emul Luterne POC Project Contact Parts-Countember Companying Call for Transassa Call for Transassa Budrassan Requirements Budrassan Requirements Evaluation Criteria Evaluation Criteria Evaluation Criteria Evaluation Criteria Evaluation Criteria	OST-CUANTUM CRYPTO STANDARDIZATION PAGNET FOR Comments On Submission Requirements And Requirements on Pagnetic	dy ing
		Ocaments Decements Federal Register Notes Enders Register Notes POC Project Contact Co	OST-CUANTUM CRYPTO STANDARDIZATION PAGNET FOR Comments On Submission Requirements And Requirements on Pagnetic	dy ing
		Ocaments Decements Federal Register Notes Enders Register Notes POC Project Contact Co	OST-CUANTUM CRYPTO STANDARDIZATION PAGNET FOR Comments On Submission Requirements And Requirements on Pagnetic	dy ing
		Ocaments Decements Federal Register Notes Enders Register Notes POC Project Contact Co	OST-CUANTUM CRYPTO STANDARDIZATION PAGNET FOR Comments On Submission Requirements And Requirements on Pagnetic	dy ing
		Ocaments Decements Federal Register Notes Enders Register Notes POC Project Contact Co	OST-CUANTUM CRYPTO STANDARDIZATION PAGNET FOR Comments On Submission Requirements And Requirements on Pagnetic	dy ing
		Ocaments Decements Federal Register Notes Enders Register Notes POC Project Contact Co	OST-CUANTUM CRYPTO STANDARDIZATION PAGNET FOR Comments On Submission Requirements And Requirements on Pagnetic	dy ing
		Ocaments Decements Federal Register Notes Enders Register Notes POC Project Contact Co	OST-CUANTUM CRYPTO STANDARDIZATION PAGNET FOR Comments On Submission Requirements And Requirements on Pagnetic	dy ing
		Ocaments Decements Federal Register Notes Enders Register Notes POC Project Contact Co	OST-CUANTUM CRYPTO STANDARDIZATION PAGNET FOR Comments On Submission Requirements And Requirements on Pagnetic	dy ing
		Ocaments Decements Federal Register Notes Enders Register Notes POC Project Contact Co	OST-CUANTUM CRYPTO STANDARDIZATION PAGNET FOR Comments On Submission Requirements And Requirements on Pagnetic	dy ing
		Ocaments Decements Federal Register Notes Enders Register Notes POC Project Contact Co	OST-CUANTUM CRYPTO STANDARDIZATION PAGNET FOR Comments On Submission Requirements And Requirements on Pagnetic	dy ing

Sara J. Ker NIST 301-975-4634 sara@nist.gov