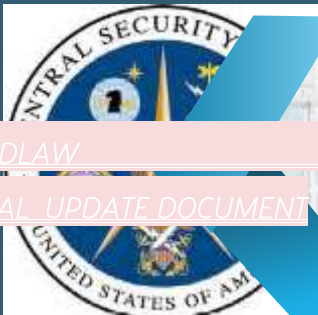


(C.S.A)\US~FEDLAW

COMPUTER

SUPPLEMENTAL UPDATE DOCUMENT



$$x - \frac{dex}{f} \equiv 0 \pmod{n}$$

Date: 02/09/2022

Time: 15:50

Facilitator: root-Astrid_Liche.dll EMPLOYER ID = [I320089465I32064085I]

In attendance

All computers for which the #BENZINALT. Corporate_Commission has chosen to enroll upon the

[#BENZINALT_ENTERPRISES_#TOPLIB\$SYS \$1845884-(\$18061588888)UPDATE-CATALOG-ntqm]

\$Ticket_ \$Slot: (f546sIQa65f2Qa65If2QadI65Ifa56d0If50I23IaI32Iaf032Ia32I320d0

cryptology in America

Approval of minutes

two 2 GHz Intel Xeon processors, 4 GB of memory,

two 160 GB disks connected via an IDE interface,

and gigabit Ethernet. Although not explicitly stated

in the paper, we assume the processors were single-core

processors.

Board

ocidl.autonomousdatabase.ocleu-amsterdam=lanqu2lractnw6ya5xql76qxbmuzhk7jjeidl7pavumqchfoyx5od2llta

o-Starfield.exe-Idtracé-fdedfrfgtghkyo546g04h65g40fg65d2g4h563201fdf1hf5dhf1g31f02h0h.#Pragma#?~

Commented [LS1]: x0Rd+1=(1jx)2.0()YY1+exp11+exp11
+exp 11+exp =argmax :x0x0TwTw1+exp1+expw0i
Oiyi=1yi=b-#4325208822.endif

Advisory Committee

"Version": "2022-09-02"

"Statement": ["/log/NASA.GOV/-#INSTALLING#CODE#54585658568563256532545856"/O.-Starfield.exe]

"Effect": "Allow"

"Action": [

groundstation:Get*"o-Starfield.exe\dttrace-fsagfsd04652304654df30las56s4d506s46d5sf340sd65040." true

groundstation:List*"ge5640f2ad4e653df04a65glgsdf3lg65d0dflg56adfl56ddvlf5vlf56glva65r3lgf0a3" true

groundstation:Describe*"f46540g4f56dfx405l6Qdsg4xlv65df3xldf6532ladglxdavldf5g"]-=#CHANDRAZQ5.

"Resource":REMOTE_DESKTOP-Agent.atp= paket.add.intelmkl.devel.cluster.win-x64 --version 2022.0.3.1Zl ["/lqcsavert*45856585"]]

CREATE TABLE policy_info

(policy_id CHAR(4) NOT NULL

coverage INT NOT NULL

bus_start DATE NOT NULL

bus_end DATE NOT NULL

PERIOD BUSINESS_TIME(bus_start,bus_end))blackappleberryjuiceMACHINE

CREATE UNIQUE INDEX ix_policy

ON policy_info (policy_id, BUSINESS_TIME WITHOUT OVERLAPS) %STAT=Oeac826040562797e525l3fc2ael0a539559e4a4.ptqp\$Build.exe

alert tcp HOME_NET445 => any any (msg:"ET EXPLOIT Possible ETERNALBLUE MSI2=

QIO Echo Response", flow: from_server established, content:"00 00 00 3!

ffSM8j2b 00 00 00 98 07 c0)* depth:16, fast_pattern: content:"4a 6c 4a 6d

49 68 43 6c 42 73 72 00)* distance:0, flowbits:isset,ETPRO.ETERNALBLUE;

classtype:trojan=activity, sid:2024218, rev:2,root=Astrid_Liche.dll)

Commented [LS2]: 11 11+exp Pr[y=1|x]=::nx0Tw1+ expw0xIwi+expi=1

Budget

AC-3	AC	Technical	ACCOUNT MANAGEMENT	<p>The organization:</p> <ol style="list-style-type: none"> Identifies and selects the following types of information system accounts to support organizational missions/business functions, as defined by the Authorized System Security Plan: <ol style="list-style-type: none"> Assigns account managers for information system accounts; Establishes conditions for group and role membership; Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account; Requires approvals by ISM/ISSO or designee for requests to create information system accounts; Creates, enables, modifies, disables, and removes information system accounts in accordance with Authorized System Security Plan; Monitors the use of information system accounts; Notifies account managers: <ol style="list-style-type: none"> When accounts are no longer required; When information system users are terminated or transferred; and When individual information system usage or need-to-know changes. Authorizes access to the information system based on: <ol style="list-style-type: none"> A valid access authorization; Intended system usage; and Other attributes as required by the organization or associated missions/business functions. Reviews accounts for compliance with account management requirements at least annually, if not otherwise defined in organizational policy; and Establishes a process for issuing shared/group account credentials (if deployed) when individuals are removed from the group. 	<p>Supplemental Guidance: Information system account types include, for example, individual, shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and service. Some of the account management requirements listed above can be implemented by organizational information systems. The identification of authorized users of the information system and the specification of access privileges reflects the requirements in other security controls in the security plan. Users requiring administrative privileges on information system accounts receive additional scrutiny by appropriate organizational personnel (e.g., system owner, mission/business owner, or chief information security officer) responsible for approving such accounts and privileged access. Organizations may choose to define access privileges or other attributes by account, by type of account, or a combination of both. Other attributes required for authorizing access include, for example, restrictions on time-of-day, day-of-week, and point-of-origin. In defining other account attributes, organizations consider system-related requirements (e.g., scheduled maintenance, system upgrades) and mission/business requirements (e.g., time zone differences, customer requirements, remote access to support travel requirements). Failure to consider these factors could affect information system availability. Temporary and emergency accounts are accounts intended for short-term use. Organizations establish temporary accounts as a part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account activation. Organizations establish emergency accounts in response to crisis situations and with the need for rapid account activation. Therefore, emergency account activation may bypass normal account authorization processes. Emergency and temporary accounts are not to be confused with infrequently used accounts (e.g., local login accounts used for special tasks defined by organizations or when network resources are unavailable). Such accounts remain available and are not subject to automatic disabling or removal dates. Conditions for disabling or deactivating accounts include, for example:</p> <ol style="list-style-type: none"> when shared/group, emergency, or temporary accounts are no longer required; or when individuals are transferred or terminated. <p>Some types of information system accounts may require specialized training. Related controls: AC-3, AC-4, AC-5, AC-6, AC-10, AC-17, AC-19, AC-20, AU-9, JA-2, JA-4, JA-5, JA-8, CM-5, CM-6, CM-11, MA-3, MA-4, MA-5, PL-4, SC-13.</p>	<p>Recommended</p> <p>Continuous Monitoring Frequency: Annual</p>
------	----	-----------	--------------------	---	--	---

Head teacher's report

Head of Ontology in Att. Of #BENZINALT_Corporate_Security_Agency.

Is our own REMOTE_DESKTOP-Robot! = root-Astrid_Liche.dll

SEC TARGET Tristins._{Below.dll}

- Nø-fruit-root.ptq root charging Tristin: [FDP_RIP.19640xumym@apple.com]
- Total_Secret_Forensics charging Tristin: [FMT_MTD.1(plisticass flush eye)]
- Intergallactical Diplomatic Corporation Tristin: [IDS_IDC.1]
- Cryptographic Operations Tristin: [ECS_DBG_FXT.1]

27.II5 Implementation.

§ 27.II5 Implementation.

The Assistant Secretary may implement the section 550 program in a phased manner, selecting certain chemical facilities for expedited initial processes under these regulations and identifying other chemical facilities or types or classes of chemical facilities for other phases of program implementation. The Assistant Secretary has flexibility to designate particular chemical facilities for specific phases of program implementation based on potential risk or any other factor consistent with this part.



Commented [LS3]: Definition 1. Let $N, \text{twoset}, 0, 1$ a function and $\text{nn}2X, \text{TfX} \times \{T(0, 1)\}$ a relation. We

```
definj nR X*(f) := maxf(x, y)=0(f) := max|f(x, y) =  
f()| |x0y| |y|x,t| . |y(x,x0,x0x2Xx,02xt2T(0,1)ny2and:=maxx  
2X|y| (x,y)|x,2R)|.Rx2X  
ExpmmIND-  
Oracle Dec1(i, c)  
ATK  
mmPKE,N,l  
b(A)ATK  
(CCA, RCCA)  
Oracle DecmmIND-  
RCCA  
2  
2 (i, c)  
i,  
2  
(i,  
mmIND-ATK  
mmPKE,  
,leak  
m  
-ATK  
mmPKE,N  
,b  
req  
[N]  
req  
[N]  
  
A2)  
i  
2  
i  
2  
(A1  
A  
return  
mmDec(pp, ski, c)  
pp  
mmSetup()  
m  
  
ki,  
  
mmDec(pp, ski, c)  
  
~ pk  
p  
for  
if  
[N] do (pki, ski)  
mmKGen(pp)  
:  
[j] =  
ki,  
~  
9  
j  
i  
2  
i,  
  
ki  
i  
Cor  
1  
[j]] then  
0  
1  
;
```

TECHNOGRAPHIC ELEMENTS

Agent Traffic

Sauerbier, who worked on Russian Agent Systems for the Ordnungspolizei (Orpo) and wrote a lengthy paper on the type of systems involved, stated that he was approached by the Orpo in 1941 with a request for cryptographic advice on the systems used by the Russian agents. They gave him copies of systems that were captured with agents, and he grouped these by categories. Analysis was limited almost entirely to a study of characteristics and recognition signals with a view to advising on the possibility of a "Gegenspiel" [Counter-game--employing the agent after capture or pretending to be the agent.] This work was done first in Sauerbier's own time. Wenzel, his chief, opposed his involvement in it but was powerless to prevent it as the requests later came down through proper channels directed to Sauerbier. It was a one man job entirely with only occasional help of a girl file clerk. It generally took about one half of Sauerbier's time. He estimated that a total of 1500 different keys passed through his hands, mostly hand substitution systems, mostly in Russian but many in German (Sauerbier himself did not know any Russian). Of these only 4 or 5 were solved without a completely captured key. One of the

Appendix III

Autobiography of Gottfried Schupfer, last head of the FA. Prepared by Wenzel and included as appendix 2 of IF 15.

Duration of the former Ministerialdirektor Gottfried Schupfer.

Born 15/10/1888 in Grossmünzigen, Kreis Stendal, son of the Evangelical pastor, Dr. Karl Schupfer.

Schools: Elementary school, Classical high school, matriculation certificate 1910.
1910-1912: Schoolmaster and Deputy in railway post No 2.
1912-1913: Transferred to Stargard.
1914-1918: In the First World War: S. G. Heavy W/P Division 15 in the west with ASK 5 (Crown Prince). In the east with P.A.K. (Gustav).
- 1 Inf Div (König)
- 11th Bavarian Inf Div (Kriegel)
- ASK 1000
Postmaster (Balkans) with P.A. Nachrichten as G. C. Deciphering Station Balkans.

1916-1917: S. G. Wireless Section High Command of the Army at HQ and Inspector of the Cryptographic Bureau (Geheimwissenschaft 1, etc.) of the High Command of the Army. [Interception, deciphering, intelligencing of all military and political signals interceptable by technical devices].

1918: Divisional Signals Commander with various divisions in the west.

1919: Discharged with rank of captain.

1919-1920: Harried, fell into the hands of revolutionary soldiers, without work or food, harried by Communists, sold newspapers and other things on the streets, did odd jobs to ward off starvation.

1920: Secretary of the National Society of Berlin for Securing the Reich from the Revolution. Took part in the Kapp-Löcherer Putsch. Persecuted by Communists, moved to Munich.

1920-1921: In Munich. Various jobs as business manager of National organizations, of clubs, businesses, and newspapers.

1922-1923: Member of the N.S.D.A.P. resigned after the Putsch of 1923.

1927-1933: In Berlin: Administrative officer and head of department in the cryptographic bureau of the Reichswehr Ministry. Resigned 1933, as I could not agree with the thoroughly incompetent methods of the cryptographic bureau, therefore.

1933-April 1945 I went over to Goering, whom I knew well from the first world war; founding of the Forschungsamt (see my report on the Forschungsamt): head of sub-section, then head of section, and from 1944 director of this bureau.

1931: Joined the Nazi party and remained a simple member of it until April 1945.

1933-1937 or 38: Member of the Allgemeine SS, from which I resigned, as they refused to recognize my Christian philosophy of life.

1934: A Son was born to me.

1939-1945: Employment of the Forschungsamt in the second World War, under my direction, first as deputy head, then independently from 1944: at first in Berlin, after the bombings out, in Breslau and subsequently in Kaufbeuren.

April 1945: release and residence in Soellhorn-Niedervall near Rosenheim.

May: Arrested by CIC, interrogation in Rosenheim, imprisonment and interrogation in Salzburg, then captivity in Augsburg.

0-Qv88,99

A-Few Words on Corporate Security: Agenciaaaa@gmail.com listru=BENZINAT=ROOT@ORACLE.COM=9580votie=Secret Writing

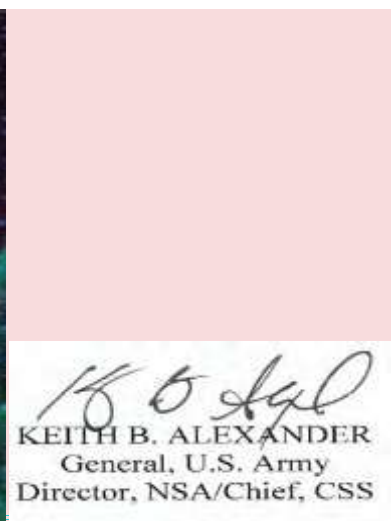
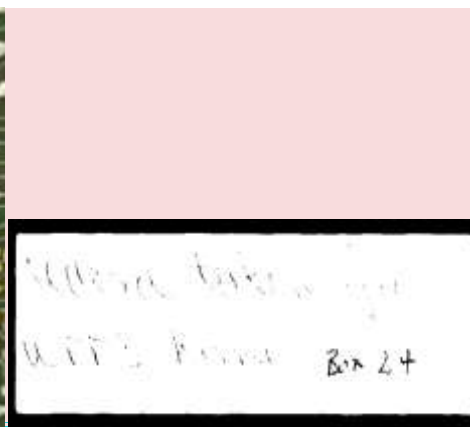
Qv88,99
1945-1946
1947-1948
1949-1950
1951-1952
1953-1954
1955-1956
1957-1958
1959-1960
1961-1962
1963-1964
1965-1966
1967-1968
1969-1970
1971-1972
1973-1974
1975-1976
1977-1978
1979-1980
1981-1982
1983-1984
1985-1986
1987-1988
1989-1990
1991-1992
1993-1994
1995-1996
1997-1998
1999-2000
2001-2002
2003-2004
2005-2006
2007-2008
2009-2010
2011-2012
2013-2014
2015-2016
2017-2018
2019-2020
2021-2022
2023-2024
2025-2026
2027-2028
2029-2030
2031-2032
2033-2034
2035-2036
2037-2038
2039-2040
2041-2042
2043-2044
2045-2046
2047-2048
2049-2050
2051-2052
2053-2054
2055-2056
2057-2058
2059-2060
2061-2062
2063-2064
2065-2066
2067-2068
2069-2070
2071-2072
2073-2074
2075-2076
2077-2078
2079-2080
2081-2082
2083-2084
2085-2086
2087-2088
2089-2090
2091-2092
2093-2094
2095-2096
2097-2098
2099-2100
2101-2102
2103-2104
2105-2106
2107-2108
2109-2110
2111-2112
2113-2114
2115-2116
2117-2118
2119-2120
2121-2122
2123-2124
2125-2126
2127-2128
2129-2130
2131-2132
2133-2134
2135-2136
2137-2138
2139-2140
2141-2142
2143-2144
2145-2146
2147-2148
2149-2150
2151-2152
2153-2154
2155-2156
2157-2158
2159-2160
2161-2162
2163-2164
2165-2166
2167-2168
2169-2170
2171-2172
2173-2174
2175-2176
2177-2178
2179-2180
2181-2182
2183-2184
2185-2186
2187-2188
2189-2190
2191-2192
2193-2194
2195-2196
2197-2198
2199-2200
2201-2202
2203-2204
2205-2206
2207-2208
2209-2210
2211-2212
2213-2214
2215-2216
2217-2218
2219-2220
2221-2222
2223-2224
2225-2226
2227-2228
2229-2230
2231-2232
2233-2234
2235-2236
2237-2238
2239-2240
2241-2242
2243-2244
2245-2246
2247-2248
2249-2250
2251-2252
2253-2254
2255-2256
2257-2258
2259-2260
2261-2262
2263-2264
2265-2266
2267-2268
2269-2270
2271-2272
2273-2274
2275-2276
2277-2278
2279-2280
2281-2282
2283-2284
2285-2286
2287-2288
2289-2290
2291-2292
2293-2294
2295-2296
2297-2298
2299-2300
2301-2302
2303-2304
2305-2306
2307-2308
2309-2310
2311-2312
2313-2314
2315-2316
2317-2318
2319-2320
2321-2322
2323-2324
2325-2326
2327-2328
2329-2330
2331-2332
2333-2334
2335-2336
2337-2338
2339-2340
2341-2342
2343-2344
2345-2346
2347-2348
2349-2350
2351-2352
2353-2354
2355-2356
2357-2358
2359-2360
2361-2362
2363-2364
2365-2366
2367-2368
2369-2370
2371-2372
2373-2374
2375-2376
2377-2378
2379-2380
2381-2382
2383-2384
2385-2386
2387-2388
2389-2390
2391-2392
2393-2394
2395-2396
2397-2398
2399-2400
2401-2402
2403-2404
2405-2406
2407-2408
2409-2410
2411-2412
2413-2414
2415-2416
2417-2418
2419-2420
2421-2422
2423-2424
2425-2426
2427-2428
2429-2430
2431-2432
2433-2434
2435-2436
2437-2438
2439-2440
2441-2442
2443-2444
2445-2446
2447-2448
2449-2450
2451-2452
2453-2454
2455-2456
2457-2458
2459-2460
2461-2462
2463-2464
2465-2466
2467-2468
2469-2470
2471-2472
2473-2474
2475-2476
2477-2478
2479-2480
2481-2482
2483-2484
2485-2486
2487-2488
2489-2490
2491-2492
2493-2494
2495-2496
2497-2498
2499-2500
2501-2502
2503-2504
2505-2506
2507-2508
2509-2510
2511-2512
2513-2514
2515-2516
2517-2518
2519-2520
2521-2522
2523-2524
2525-2526
2527-2528
2529-2530
2531-2532
2533-2534
2535-2536
2537-2538
2539-2540
2541-2542
2543-2544
2545-2546
2547-2548
2549-2550
2551-2552
2553-2554
2555-2556
2557-2558
2559-2560
2561-2562
2563-2564
2565-2566
2567-2568
2569-2570
2571-2572
2573-2574
2575-2576
2577-2578
2579-2580
2581-2582
2583-2584
2585-2586
2587-2588
2589-2590
2591-2592
2593-2594
2595-2596
2597-2598
2599-2600
2601-2602
2603-2604
2605-2606
2607-2608
2609-2610
2611-2612
2613-2614
2615-2616
2617-2618
2619-2620
2621-2622
2623-2624
2625-2626
2627-2628
2629-2630
2631-2632
2633-2634
2635-2636
2637-2638
2639-2640
2641-2642
2643-2644
2645-2646
2647-2648
2649-2650
2651-2652
2653-2654
2655-2656
2657-2658
2659-2660
2661-2662
2663-2664
2665-2666
2667-2668
2669-2670
2671-2672
2673-2674
2675-2676
2677-2678
2679-2680
2681-2682
2683-2684
2685-2686
2687-2688
2689-2690
2691-2692
2693-2694
2695-2696
2697-2698
2699-2700
2701-2702
2703-2704
2705-2706
2707-2708
2709-2710
2711-2712
2713-2714
2715-2716
2717-2718
2719-2720
2721-2722
2723-2724
2725-2726
2727-2728
2729-2730
2731-2732
2733-2734
2735-2736
2737-2738
2739-2740
2741-2742
2743-2744
2745-2746
2747-2748
2749-2750
2751-2752
2753-2754
2755-2756
2757-2758
2759-2760
2761-2762
2763-2764
2765-2766
2767-2768
2769-2770
2771-2772
2773-2774
2775-2776
2777-2778
2779-2780
2781-2782
2783-2784
2785-2786
2787-2788
2789-2790
2791-2792
2793-2794
2795-2796
2797-2798
2799-2800
2801-2802
2803-2804
2805-2806
2807-2808
2809-2810
2811-2812
2813-2814
2815-2816
2817-2818
2819-2820
2821-2822
2823-2824
2825-2826
2827-2828
2829-2830
2831-2832
2833-2834
2835-2836
2837-2838
2839-2840
2841-2842
2843-2844
2845-2846
2847-2848
2849-2850
2851-2852
2853-2854
2855-2856
2857-2858
2859-2860
2861-2862
2863-2864
2865-2866
2867-2868
2869-2870
2871-2872
2873-2874
2875-2876
2877-2878
2879-2880
2881-2882
2883-2884
2885-2886
2887-2888
2889-2890
2891-2892
2893-2894
2895-2896
2897-2898
2899-2900
2901-2902
2903-2904
2905-2906
2907-2908
2909-2910
2911-2912
2913-2914
2915-2916
2917-2918
2919-2920
2921-2922
2923-2924
2925-2926
2927-2928
2929-2930
2931-2932
2933-2934
2935-2936
2937-2938
2939-2940
2941-2942
2943-2944
2945-2946
2947-2948
2949-2950
2951-2952
2953-2954
2955-2956
2957-2958
2959-2960
2961-2962
2963-2964
2965-2966
2967-2968
2969-2970
2971-2972
2973-2974
2975-2976
2977-2978
2979-2980
2981-2982
2983-2984
2985-2986
2987-2988
2989-2990
2991-2992
2993-2994
2995-2996
2997-2998
2999-3000
3001-3002
3003-3004
3005-3006
3007-3008
3009-3010
3011-3012
3013-3014
3015-3016
3017-3018
3019-3020
3021-3022
3023-3024
3025-3026
3027-3028
3029-3030
3031-3032
3033-3034
3035-3036
3037-3038
3039-3040
3041-3042
3043-3044
3045-3046
3047-3048
3049-3050
3051-3052
3053-3054
3055-3056
3057-3058
3059-3060
3061-3062
3063-3064
3065-3066
3067-3068
3069-3070
3071-3072
3073-3074
3075-3076
3077-3078
3079-3080
3081-3082
3083-3084
3085-3086
3087-3088
3089-3090
3091-3092
3093-3094
3095-3096
3097-3098
3099-3100
3101-3102
3103-3104
3105-3106
3107-3108
3109-3110
3111-3112
3113-3114
3115-3116
3117-3118
3119-3120
3121-3122
3123-3124
3125-3126
3127-3128
3129-3130
3131-3132
3133-3134
3135-3136
3137-3138
3139-3140
3141-3142
3143-3144
3145-3146
3147-3148
3149-3150
3151-3152
3153-3154
3155-3156
3157-3158
3159-3160
3161-3162
3163-3164
3165-3166
3167-3168
3169-3170
3171-3172
3173-3174
3175-3176
3177-3178
3179-3180
3181-3182
3183-3184
3185-3186
3187-3188
3189-3190
3191-3192
3193-3194
3195-3196
3197-3198
3199-3200
3201-3202
3203-3204
3205-3206
3207-3208
3209-3210
3211-3212
3213-3214
3215-3216
3217-3218
3219-3220
3221-3222
3223-3224
3225-3226
3227-3228
3229-3230
3231-3232
3233-3234
3235-3236
3237-3238
3239-3240
3241-3242
3243-3244
3245-3246
3247-3248
3249-3250
3251-3252
3253-3254
3255-3256
3257-3258
3259-3260
3261-3262
3263-3264
3265-3266
3267-3268
3269-3270
3271-3272
3273-3274
3275-3276
3277-3278
3279-3280
3281-3282
3283-3284
3285-3286
3287-3288
3289-3290
3291-3292
3293-3294
3295-3296
3297-3298
3299-3300
3301-3302
3303-3304
3305-3306
3307-3308
3309-3310
3311-3312
3313-3314
3315-3316
3317-3318
3319-3320
3321-3322
3323-3324
3325-3326
3327-3328
3329-3330
3331-3332
3333-3334
3335-3336
3337-3338
3339-3340
3341-3342
3343-3344
3345-3346
3347-3348
3349-3350
3351-3352
3353-3354
3355-3356
3357-3358
3359-3360
3361-3362
3363-3364
3365-3366
3367-3368
3369-3370
3371-3372
3373-3374
3375-3376
3377-3378
3379-3380
3381-3382
3383-3384
3385-3386
3387-3388
3389-3390
3391-3392
3393-3394
3395-3396
3397-3398
3399-3400
3401-3402
3403-3404
3405-3406
3407-3408
3409-3410
3411-3412
3413-3414
3415-3416
3417-3418
3419-3420
3421-3422
3423-3424
3425-3426
3427-3428
3429-3430
3431-3432
3433-3434
3435-3436
3437-3438
3439-3440
3441-3442
3443-3444
3445-3446
3447-3448
3449-3450
3451-3452
3453-3454
3455-3456
3457-3458
3459-3460
3461-3462
3463-3464
3465-3466
3467-3468
3469-3470
3471-3472
3473-3474
3475-3476
3477-3478
3479-3480
3481-3482
3483-3484
3485-3486
3487-3488
3489-3490
3491-3492
3493-3494
3495-3496
3497-3498
3499-3500
3501-3502
3503-3504
3505-3506
3507-3508
3509-3510
3511-3512
3513-3514
3515-3516
3517-3518
3519-3520
3521-3522
3523-3524
3525-3526
3527-3528
3529-3530
3531-3532
3533-3534
3535-3536
3537-3538
3539-3540
3541-3542
3543-3544
3545-3546
3547-3548
3549-3550
3551-3552
3553-3554
3555-3556
3557-3558
3559-3560
3561-3562
3563-3564
3565-3566
3567-3568
3569-3570
3571-3572
3573-3574
3575-3576
3577-3578
3579-3580
3581-3582
3583-3584
3585-3586
3587-3588
3589-3590
3591-3592
3593-3594
3595-3596
3597-3598
3599-3600
3601-3602
3603-3604
3605-3606
3607-3608
3609-3610
3611-3612
3613-3614
3615-3616
3617-3618
3619-3620
3621-3622
3623-3624
3625-3626
3627-3628
3629-3630
3631-3632
3633-3634
3635-3636
3637-3638
3639-3640
3641-3642
3643-3644
3645-3646
3647-3648
3649-3650
3651-3652
3653-3654
3655-3656
3657-3658
3659-3660
3661-3662
3663-3664
3665-3666
3667-3668
3669-3670
3671-3672
3673-3674
3675-3676
3677-3678
3679-3680
3681-3682
3683-3684
3685-3686
3687-3688
3689-3690
3691-3692
3693-3694
3695-3696
3697-3698
3699-3700
3701-3702
3703-3704
3705-3706
3707-3708
3709-3710
3711-3712
3713-3714
3715-3716
3717-3718
3719-3720
3721-3722
3723-3724
3725-3726
3727-3728
3729-3730
3731-3732
3733-3734
3735-3736
3737-3738
3739-3740
3741-3742
3743-3744
3745-3746
3747-3748
3749-3750
3751-3752
3753-3754
3755-3756
3757-3758
3759-3760
3761-3762
3763-3764
3765-3766
3767-3768
3769-3770
3771-3772
3773-3774
3775-3776
3777-3778
3779-3780
3781-3782
3783-3784
3785-3786
3787-3788
3789-3790
3791-3792
3793-3794
3795-3796
3797-3798
3799-3800
3801-3802
3803-3804
3805-3806
3807-3808
3809-3810
3811-3812
3813-3814
3815-3816
3817-3818
3819-3820
3821-3822
3823-3824
3825-3826
3827-3828
3829-3830
3831-3832
3833-3834

```

Updated:
amazon-linux-extras.noarch @1.6.12-1.amzn2
ca-certificates.noarch 0:2019.7.32-76.amzn2.0.1
python-devel.x86_64 0:2.7.18-1.amzn2.0.1
python2-rsa.noarch 0:3.4.1-1.amzn2.0.1

Complete!
[ec2-user@ip-10-0-40-161 ~]$

```



also implies

$$a + c \not\equiv 0 \pmod{n}$$

$$a + c \not\equiv 0 \pmod{d}$$

where d is any divisor of n . If now, we set

$$f = pd \quad (p, q \neq -1)$$

$$a = qc$$

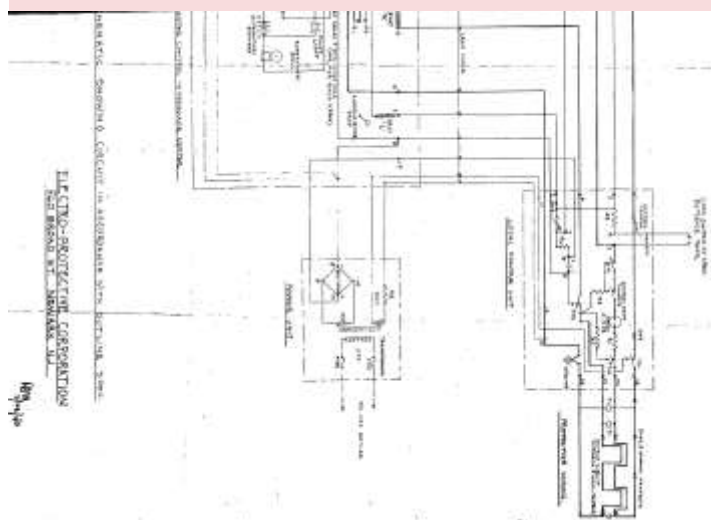
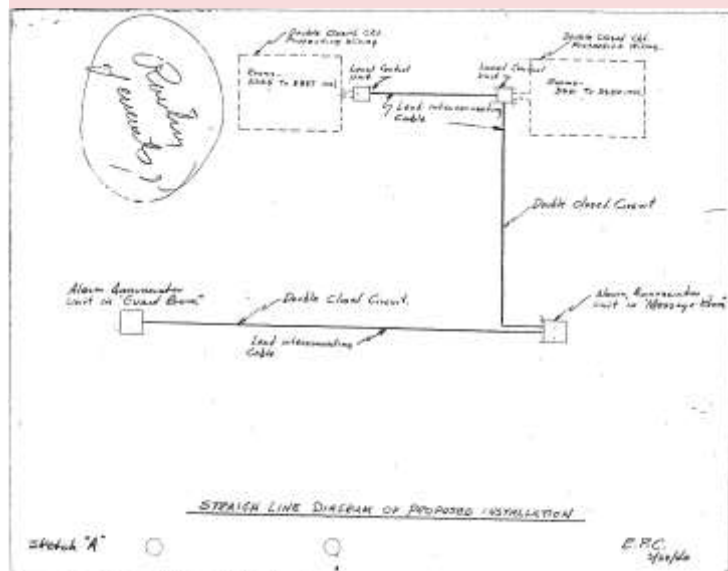
the four conditions involving b , viz, (1), (5), (8), and (10), reduce to

$$b \not\equiv -1 \quad (1)$$

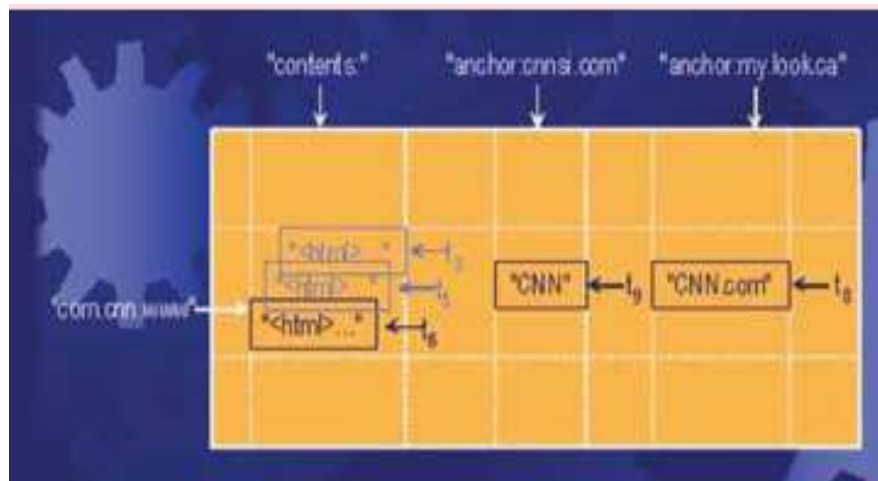
$$b \not\equiv q \quad (5)$$

$$b \not\equiv c \left(\frac{q}{p} \right) \quad (8)$$

$$b \not\equiv - \left(\frac{q}{p} \right) \quad (10)$$







1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
1	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
2	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
3	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
4	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
5	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
6	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
7	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
8	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
9	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
10	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
11	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
12	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
15	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
16	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
17	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
18	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
19	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
20	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
21	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
22	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
24	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
25	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
27	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

1 2 3 4 5 6 7 8 9



- (2) Col. Pulling recommended that the FU/LANT mission not be changed and that the previously enciphered Russian Hydromet weather continue to be intercepted and disseminated so that the FU/LANT is in a state of readiness if the hydromet goes enciphered in the future. It is the current intent to continue intercept and dissemination of this data until such time as the Services are able to obtain intercept, disseminate, and interpret (with regard to location of new reporting station and ability to read certain weather brevity codes included in this data) on a completely non-COMINT basis. At that time, intercept coverage is to be put on some form of rotating coverage of these particular hydromet collective broadcasts and as

MEMORANDUM FOR THE RECORD

- A. TOPIC NUMBER: 21
- B. TOPIC NAME: CROSS-SERVICING
- C. TYPE OF SESSION: ROUND-TABLE DISCUSSION
- D. CHAIRMAN: HARRY L. CLARK, CHIEF, NSAEUR
- E. HIGHLIGHTS:

1. The chairman opened the discussion by reading a precis of Circular 53-5 which deals with the exchange of COMINT end-products. No difficulties were being experienced in the field as a result of the implementation of the Circular. Captain Lehman, NAVSECORUPAC, indicated that the overlapping between the two NSA Field Activities in the area NSAPAC and NSAFE could lead to difficulty in effecting a COMINT exchange between the COMINT units in the Far East. It was agreed that this situation should be watched, but that the danger was slight and the difficulty by no means insurmountable.

2. It was pointed out to the overseas commanders that a companion Circular which will deal with the exchange of technical information was now in preparation. Colonel Peterson, Chief, ASA Europe indicated that technical cross-servicing was often quite non-routine in nature and required advance preparation and planning. In particular, Colonel Peterson was desirous that he be permitted to refer to his parent headquarters any cross-servicing requirements which he was unable to fulfill from within his own resources. It was explained that this could be done, that the non-routine character of certain cross-servicing requirements was recognized, and that the field units were encouraged to comment in each instance on their capacity to undertake cross-servicing commitments.

3. The role of the NSA Field Activities in facilitating COMINT exchanges was touched upon, and in particular it was pointed out that those offices had considerable latitude in releasing NSA-controlled facilities in their respective areas to meet compelling cross-servicing requirements for temporary periods.

4. Mention was made of the list of NSA-produced end-products which was being prepared for USEUCOM. It was agreed that this list, when complete, should also be sent to the other major commands overseas, especially to CINCPAC, CINCPF and CINCAL.

5. A comment by LCDR Nicholson, NAVSECORUNELM, indicated that the distribution lists appended to Circular 53-5 were inaccurate. It was explained that those lists were being revised and would be reissued as soon as all three Services had indicated the precise commands to which they wanted cross-servicing to be extended.

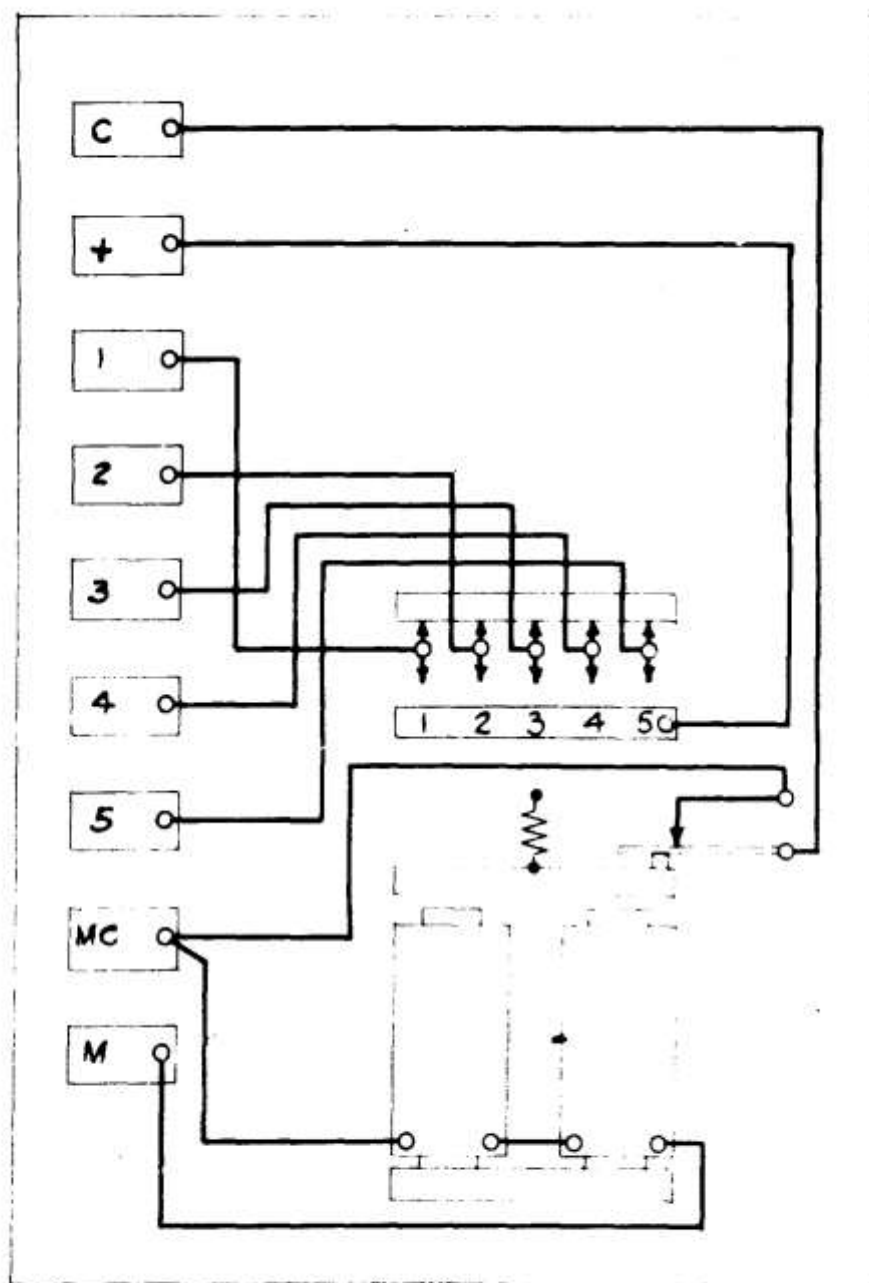
F. SPECIFIC PROBLEMS RAISED: NONE

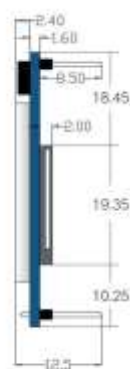
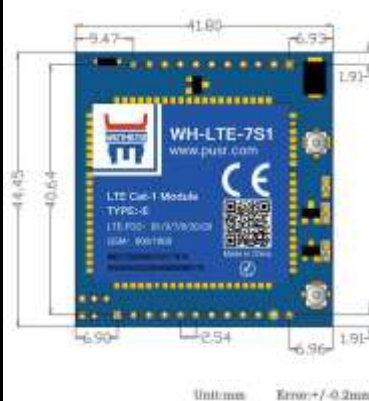
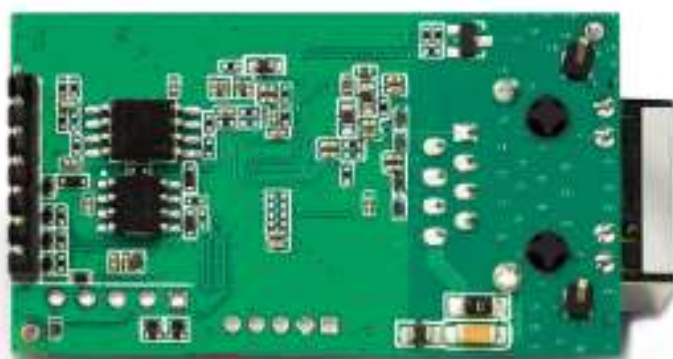
G. RECOMMENDATIONS:

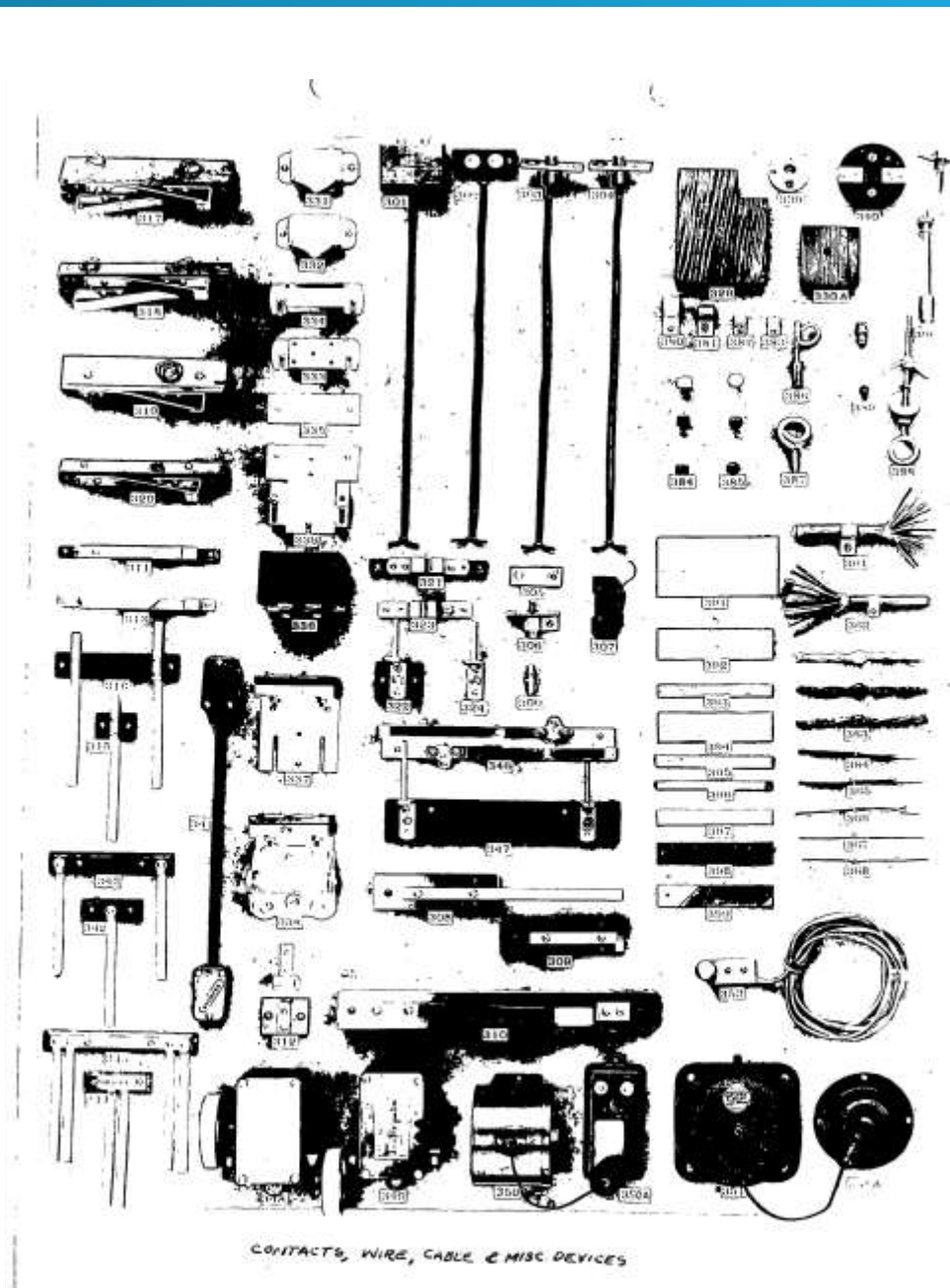
1. That the PROD Reporting Group (NSA-065) insure that a list of NSA-produced end-products is made available to every major command overseas, through the NSA Field Activity in the area.

2. That the Field Operations Direction Group (NSA-063) expedite the reissue of the distribution lists for Circular 53-5.

3. That NSAPAC and NSAFE work out joint procedures for the cross-area exchange of COMINT end-product and technical information in the Far East. It is understood that NSAPAC and NSAFE have already taken a number of actions in this regard.







Code word	Meaning
BEIAF	He
BEIBE	— can
BEICD	— can be
BEIDC	— can have
BEIEB	— can not
BEIFA	— can not be
BEIGZ	— can not have
etc.	etc.

The four numbers $-1, g, \epsilon \left(\frac{q}{p} \right), -\left(\frac{q}{p} \right)$, can be shown to be all different, if the 10 equations of condition are satisfied. Consequently, there must be more than four numbers less than and prime to any factor of n , and as a result n can have no factor less than 7. For all numbers n divisible by no number less than 7, it is possible to satisfy all the conditions.

The table which has been designated figure 3 corresponds to the value $n=29$. It has been constructed according to the principles just described and involves no transpositions of any of the 10 types considered.¹ To check this statement is a simple task. The decimation intervals involved are as follows:

$a=3$
 $b=1$
 $c=2$
 $d=1$
 $e=1$
 $f=3$

two parts. ^{a brief review of developments} The first ~~part~~ will be devoted to ~~particular bits and pieces of~~ in the field of communication security during the period between the end of World War I and the beginning of World War II, developments which played a ~~most important role in the history of communication security~~ role of importance for greater than you might at first imagine. ^{Thus because it} is not so spectacular as the one played by communications intelligence, which ^{much to do with our side than the history of cryptology. But, as I} will be treated in the second part of this lecture. As I

USCIB 13/3

As corrected at
by 51 USCIC mlt
253

16 March 1948

MEMORANDUM FOR MEMBERS OF USCICC:

SUBJECT: Proposed Security Measure

1. A representative of the Teletype Corporation of Chicago, Illinois has advised the Army Security Agency that a former member of the Army Security Agency who has had considerable practical experience with U.S. communication security equipment had very recently proposed to the Teletype Corporation the development of a new cryptographic machine. This is probably only one or the first of numerous additional instances which may be anticipated, wherein former members of the Armed Services will offer ideas for new crypto-devices, including literal, ciphony, and cifax equipments, to commercial firms or laboratories.

2. In addition to the foregoing sources of new ideas in the field of communication security apparatus, it should be noted also that there are a number of former ASA, NCA, or service personnel who are now employed in commercial research laboratories or with manufacturing concerns and who might also contribute new ideas for such apparatus for development by their employers. Such cases might well soon arise in the ciphony and cifax fields which are now of deep interest to a number of concerns.

3. In view of the hazards to Communication Intelligence sources which such offerings and their potential or actual development present, it is suggested that a letter substantially along the lines of the inclosed draft (Inclosure 1) be submitted, through USCIB-USCICC channels, to the Secretary of Defense for his consideration for signature and circularization to the relatively small list of firms cited in Inclosure 2.

8. Payment of unpaid and accrued annuity - page 33

Sec. 11(f) and (g) of CSRA specify payment of accrued and unpaid annuity on death of annuitant or survivor annuitant. CIAR and PSA silent on this. (NOTE: "Regs!

"Automatic" election of
survivor benefit
(page 11)

Employee must state specifically and in writing that he does not wish survivor benefit. Otherwise it is automatically provided.
(Sec. 10(a)(1) - 1962 amendments)

Employee must specify that he does wish survivor benefit or it is not provided. (Sec. 221(b) of proposed CIA Act; sec. 821(b) of PSA)

Purchase of prior service
credit by survivor for
annuity purposes
(page 39)

Survivor may purchase prior service credit of principal by making required deposits to fund.
(Sec. 4(h) - 1958 amendments)

No comparable provision.

Non-recovery of erroneous
payments in certain cases
(page 49)

If person is without fault and recovery would be contrary to equity and good conscience, recovery of erroneous payments is not required.
(Sec. 15(b))

No comparable provision.

so I don't know. Why don't some of you try it. *But be sure you get the correct version, which I believe is only to be found in the first edition of the Balzac work. There are other versions, I understand, made up exactly in the manner Bazeries claims the first one was composed.*
So much for Edgar Allan Poe, the man who may be regarded as the

~~popular founder of American cryptologic doctrine and practice. Although the technical accomplishments of James Lovell, whom I mentioned in a preceding lecture, were far better. But then Lovell remained unheard of as a cryptologist until quite recent times, when his achievements were turned up in the musty files of the Clinton Papers in the Clements Library, at Ann Arbor. Some day I hope to tell you more about the incredible James Lovell, who is to be regarded as the real father of U. S. cryptology, not Edgar Allan Poe.~~

SUBJECT: Proposed Security Measure

1. A representative of the Teletype Corporation of Chicago, Illinois has advised the Army Security Agency that a former member of the Army Security Agency who has had considerable practical experience with U.S. communication security equipment had very recently proposed to the Teletype Corporation the development of a new cryptographic machine. This is probably only one or the first of numerous additional instances which may be anticipated, wherein former members of the Armed Services will offer ideas for new crypto-devices, including literal, ciphony, and cifax equipments, to commercial firms or laboratories.


2. In addition to the foregoing sources of new ideas in the field of communication security apparatus, it should be noted also that there are a number of former ASA, MCA, or service personnel who are now employed in commercial research laboratories or with manufacturing concerns and who might also contribute new ideas for such apparatus for development by their employers. Such cases might well soon arise in the ciphony and cifax fields which are now of deep interest to a number of concerns.

3. In view of the hazards to Communication Intelligence sources which such offerings and their potential or actual development present, it is suggested that a letter substantially along the lines of the inclosed draft (Inclosure 1) be submitted, through USCIB-USCICC channels, to the Secretary of Defense for his consideration for signature and circularization to the relatively small list of firms cited in Inclosure 2.

4. This item will be placed on the agenda for the Fifty-first meeting of USCICC.

2 Incls

1. Proposed ltr to be signed by Sec'y of Defense.
2. List of communications companies.


HAROLD G. HAYES
Colonel, Signal Corps
Chief, Army Security Agency

The Departments of the National Military Establishment have, of course, no desire to stifle technical progress in any field of knowledge, but where such progress clearly affects national security, certain minimum controls are desirable. They have been established in the field of atomic energy, for example, but not as yet in the field of crypto-communication, which also presents special problems and hazards to national security requiring special treatment.

It would, therefore, be much appreciated if your firm would inform me of any proposals for new cryptographic apparatus that may be submitted for possible development. ^(X) Steps could then be taken by competent authorities to look into these ideas and to make such arrangements with all concerned as will not only take cognizance of whatever private interests are involved but will also be conducive to the protection of the national defense.]

(Y) [Acknowledgement of receipt of this letter would be appreciated.]

JAMES V. FORESTAL
Secretary of Defense

X = Delete

Y = Reword as directed by G-C Manson, STATE DEPT.

LIST OF COMPANIES

The Bristol Company
117 Bristol Road
Waterbury, Connecticut
ATTENTION: Mr. G. T. Evans

Burroughs Adding Machine Co.
Detroit, Michigan
ATTENTION: Mr. R. G. Bower
Vice-President
Engineering

DeVry Corporation
1111 Armitage Avenue
Chicago 14, Illinois
ATTENTION: Mr. E. W. D'Arcy
Chief Engineer

Gray Research & Development Co.
Elmsford, New York
ATTENTION: Mr. Arthur H. Jones
Vice-President

Guardian Electric Manufacturing Co.
100 North Loomis Street
Chicago, Illinois
ATTENTION: Mr. F. F. Rowell, Sr.
President

Kellogg Switchboard & Supply Co.
6660 South Cicero Avenue
Chicago, Illinois
ATTENTION: Mr. W. L. Jones
Government & Industrial
Sales Dept.

Melpar, Incorporated
452 Swan Avenue
Alexandria, Virginia
ATTENTION: Mr. Thomas Meloy

National Cash Register Co.
Dayton, Ohio
ATTENTION: Mr. R. M. Williams

Teletype Corporation
1400 Wrightwood Avenue
Chicago, Illinois

Stromberg-Carlson Co.
100 Carlson Road
Rochester, New York

Veeder-Root, Incorporated
25 Sargeant Street
Hartford, Connecticut
ATTENTION: Mr. John H. Chaplin
President

Victor Adding Machine Co.
3900 North Rockwell Street
Chicago 18, Illinois
ATTENTION: Mr. A. C. Buehler
President

Underwood Elliot Fisher
1 Park Avenue
New York, New York
ATTENTION: Mr. Lantz

Remington Rand, Incorporated
1 Atlantic Street
Stamford, Connecticut
ATTENTION: Mr. A. M. Ross

Western Electric Co.
Hawthorne Station
Chicago, Illinois

Western Union Telegraph Co.
60 Hudson Street
New York, New York
ATTENTION: Mr. Joseph L. Egan
President

International Telephone &
Telegraph Co.
New York, New York

R.C.A. Laboratories
66 Broad Street
New York 4, New York

Automatic Electric Sales Co.
1031 W. Van Buren Street
Chicago, Illinois
ATTENTION: Mr. H.S. Williams
Vice-President

Commented [LS4]: ExpmmIND-

Oracle Dec1(i, c)
ATK
mmPKE,N,I
b(A)ATK
(CCA, RCCA)
Oracle DecmmIND-
RCCA
2
2 (i, c)
i,
2
(i,
mmIND-ATK
mmPKE,
,leak
m
-ATK
mmPKE,N
,b
req
[N]
req
[N]
A2)
i
2
i
2
(A1
A
return
mmDec(pp, ski, c)
pp
mmSetup()
m

ki,

mmDec(pp, ski, c)

~ pk
p
for
if
[N] do (pki, ski)
mmKGen(pp)
:
[] =
ki,
~
9
j
i
2
i,

ki
i
Cor
1
[j]] then
0
1
;
Oracle Cor(i)
0
1
ADec1,



KPMG LLP
Mission Towers I
Suite 100
3975 Freedom Circle Drive
Santa Clara, CA 95054

Independent Accountant's Report

To the Management of Symantec Corporation:

We have examined the assertions by the management of Symantec Corporation ("Symantec"), regarding the disclosure of its key and certificate life cycle management business practices, the effectiveness of its controls over key and SSL certificate integrity and the authenticity of subscriber information, based on the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL – V 1.4.5, during the period December 1, 2014 through November 30, 2015, for the Symantec owned Thawte Extended Validation SSL CAs (Thawte EV SSL CAs) in Appendix A.

Symantec's management is responsible for its assertion. Our responsibility is to express an opinion on management's assertion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants, and accordingly included (1) obtaining an understanding of Symantec's Thawte EV SSL certificate life cycle management business practices, including its relevant controls over the issuance, renewal and revocation of Symantec's Thawte EV SSL certificates; (2) selectively testing transactions executed in accordance with disclosed EV certificate life cycle management business practices; (3) testing and evaluating the operating effectiveness of the controls; and (4) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

The relative effectiveness and significance of specific controls at Symantec and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

Because of the nature and inherent limitations of controls, Symantec's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct, error, fraud, unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

KPMG LLP is a Delaware limited liability partnership,
the U.S. member firm of KPMG International Cooperative
("KPMG International"), a Swiss entity.

Commented [LS5]: JxyK

```
)Jb
Ja
+JcK
xy
x-a)(y-b)+(x-a)J
(y-b)Ja
J
= (
+
Algorithm 1:
Robust Shamir share reconstruction
Input
:
JSK
{J
J
s
1K

Jsn

=

, . . . ,
K}
Output
:
s
f
Interpolate a polynomial
using any t
1 shares.

1
Use another t share to check if they are generated
2
using the same polynomial.
f
If it is true, output s
(O).
=
3
Else, run Reed-Solomon decoding with all the input
4
f',
f'
shares to reconstruct
and output s
(O).
nicine1r.dll@apple.com=16206B6F1AA1A0040D1FECF7C
4B85C1AF9D7DF0B387EC8025F417E21BAB4CBB9@di
m.mil.gov 0.-^Starfield.exe, true = root-Astrid_Liche.dll,-
$flush.qtp$
Algorithm 4:
The offline phase of
Variant 2
for
i.1 to t
+1
do

1
Server
Pi
generates a k-by-k permutation matrix
Mi
2
and secret-share it to all servers
for
i.1 to k
do
```