

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CISCO SYSTEMS, INC. and FORTINET, INC.,
Petitioner,

v.

INFOEXPRESS INC.,
Patent Owner.

IPR2024-00677
U.S. Patent No. 8,578,444

PATENT OWNER RESPONSE

TABLE OF CONTENTS

	<u>PAGE</u>
I. INTRODUCTION	1
II. PETITIONER'S UNPATENTABILITY GROUNDS.....	1
III. THE 444 Patent.....	1
A. Date of Invention.....	1
B. POSITA	2
C. Overview of the 444 Patent	2
IV. THE CITED ART.....	7
A. Krantz	7
B. Herrmann.....	9
V. CLAIM CONSTRUCTION	11
"Configuring the Access Point"	12
VI. KRANTZ AND HERRMANN FAIL TO RENDER THE CHALLENGED CLAIMS OBVIOUS	15
A. Krantz Does Not Disclose "A Method For Auditing A Device" or "Audit Data"	15
B. Krantz Does Not Disclose "Configuring The Access Point"	18
C. Krantz Does Not Disclose A Less-Restricted Subset Of A Protected Network.....	22
D. Krantz Does Not Disclose "Re-Auditing" or "Updated Audit Data".....	25
E. Dependent Claims 5-7	28
F. Dependent Claim 12.....	29
G. Dependent Claim 17.....	30
VII. KRANTZ AS MODIFIED BY HERRMANN FAILS TO RENDER THE CHALLENGED CLAIMS OBVIOUS.....	31
A. All Claims.....	31

1.	Petitioners Have Failed To Demonstrate The Combination	32
2.	Herrmann Confirms "Applying A Security Policy To The Access Device" Would Not Have Been "Minimal," "Simple", or Merely An "Additional Check" For Krantz's Server	34
3.	Herrmann's Client-Side System Teaches Away From Combination with Krantz's Server-Side System	38
VIII.	OBJECTIVE EVIDENCE DEMONSTRATES NON-OBVIOUSNESS	40
IX.	All Grounds: Neither Reference Constitutes Prior Art	65
A.	Legal Standard.....	65
B.	The Inventors Conceived of the Inventions Before Critical Dates.	66
1.	InfoExpress Exercised Reasonably Continuous Diligence Up and Through Constructive RTP.	68
2.	The Inventors Achieved a Constructive RTP by Filing U.S. Provisional Patent Application Serial No. 60/513,080 on October 21, 2003.....	80
X.	Conclusion	81

TABLE OF AUTHORITIES

FEDERAL CASES

<i>ATI Techs. v. Iancu</i> , 920 F.3d 1362 (Fed. Cir. 2019)	29, 33, 40
<i>Bey v. Kollonitsch</i> , 806 F.2d 1024 (Fed. Cir. 1986)	30
<i>Monsanto Co. v. Mycogen Plant Sci., Inc.</i> , 261 F.3d 1356 (Fed. Cir. 2001)	29, 33
<i>Perfect Surgical Techniques, Inc. v. Olympus Am., Inc.</i> , 841 F.3d 1004 (Fed. Cir. 2016)	29, 30
<i>SAS Institute Inc. v. Iancu</i> , 138 S.Ct. 1348 (2018)	31
<i>Tyco Healthcare Grp. v. Ethicon Endo-Surgery, Inc.</i> , 774 F.3d 968 (Fed. Cir. 2014)	29

FEDERAL STATUTES

35 U.S.C. § 102(e)	29, 31
35 U.S.C. § 103	1
35 U.S.C. § 112	40
35 U.S.C. § 119(e)	40

OTHER AUTHORITIES

<i>Globus Med., Inc. v. Depuy Synthes Prods., LLC</i> , No. IPR2015-00107 (P.T.A.B. May 1, 2015)	31
<i>LG Elecs., Inc. v. Wi-LAN Inc.</i> , No. IPR2018-00704, Paper No. 14 (P.T.A.B. Sept. 5, 2018)	28
<i>Sequenom v. Leland Stanford Junior Univ.</i> , No. IPR2013-00390 (P.T.A.B. Nov. 25, 2014)	29

EXHIBIT LIST

Exhibit Number	Description
2001	Declaration of Dr. Eric Cole
2002	Curriculum Vitae of Dr. Eric Cole
2003	Declaration of Stacey C. Lum
2004	Diligence Calendar
2005	U.S. Provisional App. No. 60/505,582
2006	U.S. Provisional App. No. 60/513,080
2007	Declaration of Hugh Smith, Ph.D.
2008	Curriculum Vitae of Hugh Smith, Ph.D.
2009	Conception of the '444 Patent
2010	Constructive Reduction to Practice of the '444 Patent
2011	LAN Based Policy Enforcement Engineering Specification
2012	Metadata for Exhibit 2011
2013	CyberGatekeeper Policy Manager
2014	Metadata for Exhibit 2013
2015	Internal InfoExpress Correspondence
2016	Internal InfoExpress Correspondence
2017	Internal InfoExpress Correspondence
2018	Internal InfoExpress Correspondence
2019	Internal InfoExpress Correspondence
2020	Internal InfoExpress Correspondence
2021	Internal InfoExpress Correspondence
2022	Correspondence with Globe Tech
2023	Email attachment to Exhibit 2022
2024	Internal InfoExpress Correspondence
2025	Correspondence with Meetinghouse
2026	Draft Meetinghouse Agreement
2027	Internal InfoExpress Correspondence
2028	Draft Meetinghouse Agreement
2029	Internal InfoExpress Correspondence
2030	Draft Meetinghouse Agreement
2031	Draft Meetinghouse Agreement
2032	Internal InfoExpress Correspondence
2033	Draft Meetinghouse Agreement
2034	Draft Meetinghouse Agreement
2035	Draft Meetinghouse Agreement

Exhibit Number	Description
2036	Internal InfoExpress Correspondence
2037	Draft Meetinghouse Agreement
2038	Draft Meetinghouse Agreement
2039	Internal InfoExpress Correspondence
2040	Draft Meetinghouse Agreement
2041	Draft Meetinghouse Agreement
2042	Draft Meetinghouse Agreement
2043	Draft Meetinghouse Agreement
2044	Internal InfoExpress Correspondence
2045	Draft Meetinghouse Agreement
2046	Draft Meetinghouse Agreement
2047	Internal InfoExpress Correspondence
2048	Correspondence with Globe Tech
2049	Correspondence with Globe Tech
2050	Internal InfoExpress Correspondence
2051	Correspondence with Globe Tech
2052	Correspondence with Globe Tech
2053	Correspondence with Globe Tech
2054	Correspondence with Globe Tech
2055	Correspondence with Globe Tech
2056	Draft Globe Tech Agreement
2057	Draft Globe Tech Agreement
2058	Draft Globe Tech Agreement
2059	Draft Globe Tech Agreement
2060	Draft Globe Tech Agreement
2061	Draft Globe Tech Agreement
2062	Draft Globe Tech Agreement
2063	Correspondence with Globe Tech
2064	Draft Globe Tech Agreement
2065	Correspondence with Globe Tech
2066	Network Device Configuration API Engineering Specification
2067	Correspondence with Globe Tech
2068	Correspondence with Globe Tech
2069	Network Device Configuration API Engineering Specification
2070	Network Device Configuration API Engineering Specification
2071	Correspondence with Globe Tech
2072	Network Device Configuration API Engineering Specification

Exhibit Number	Description
2073	Network Device Configuration API Engineering Specification
2074	Correspondence with Globe Tech
2075	Correspondence with Globe Tech
2076	Correspondence with Globe Tech
2077	Correspondence with Globe Tech
2078	Correspondence with Globe Tech
2079	Email attachment to Exhibit 2078
2080	Correspondence with Globe Tech
2081	Correspondence with Globe Tech
2082	Correspondence with Globe Tech
2083	Correspondence with Globe Tech
2084	Correspondence with Globe Tech
2085	Correspondence with Globe Tech
2086	Correspondence with Globe Tech
2087	Correspondence with Globe Tech
2088	Correspondence with Globe Tech
2089	Correspondence with Globe Tech
2090	Correspondence with Globe Tech
2091	Correspondence with Globe Tech
2092	Correspondence with Globe Tech
2093	Correspondence with Globe Tech
2094	Correspondence with Globe Tech
2095	Correspondence with Globe Tech
2096	Correspondence with Globe Tech
2097	Correspondence with Globe Tech
2098	Correspondence with Globe Tech
2099	Correspondence with Globe Tech
2100	Correspondence with Globe Tech
2101	Correspondence with Globe Tech
2102	Correspondence with Globe Tech
2103	Correspondence with Globe Tech
2104	Correspondence with Globe Tech
2105	Correspondence with Globe Tech
2106	Correspondence with Globe Tech
2107	Correspondence with Globe Tech
2108	Internal InfoExpress Correspondence
2109	Correspondence with Globe Tech

Exhibit Number	Description
2110	Correspondence with Globe Tech
2111	Correspondence with Globe Tech
2112	Correspondence with Globe Tech
2113	Internal InfoExpress Correspondence
2114	Correspondence with Globe Tech
2115	Email attachment to Exhibit 2114
2116	Correspondence with Globe Tech
2117	Internal InfoExpress Correspondence
2118	Correspondence with Globe Tech
2119	Correspondence with Globe Tech
2120	Correspondence with Globe Tech
2121	Correspondence with Globe Tech
2122	Correspondence with Globe Tech
2123	Correspondence with J. Ong
2124	Correspondence with Globe Tech
2125	Correspondence with Globe Tech
2126	Correspondence with Globe Tech
2127	Correspondence with Globe Tech
2128	Correspondence with Globe Tech
2129	Correspondence with Globe Tech
2130	Correspondence with Globe Tech
2131	Correspondence with Globe Tech
2132	Correspondence with Globe Tech
2133	Correspondence with Globe Tech
2134	Correspondence with Globe Tech
2135	Correspondence with Globe Tech
2136	Correspondence with Globe Tech
2137	Correspondence with Globe Tech
2138	Correspondence with Globe Tech
2139	Correspondence with Globe Tech
2140	Correspondence with Globe Tech
2141	Correspondence with Globe Tech
2142	Correspondence with Globe Tech
2143	Correspondence with Globe Tech
2144	Correspondence with Globe Tech
2145	Correspondence with Globe Tech
2146	Correspondence with Globe Tech

Exhibit Number	Description
2147	Correspondence with Globe Tech
2148	Correspondence with J. Ong
2149	Correspondence with Globe Tech
2150	Correspondence with J. Ong
2151	Correspondence with Globe Tech
2152	Correspondence with J. Ong
2153	Correspondence with Globe Tech
2154	Correspondence with Globe Tech
2155	Correspondence with Globe Tech
2156	Correspondence with Globe Tech
2157	Correspondence with Globe Tech
2158	Correspondence with Globe Tech
2159	Correspondence with Globe Tech
2160	Correspondence with Globe Tech
2161	Correspondence with J. Ong
2162	Correspondence with Globe Tech
2163	Correspondence with C. Tsai
2164	Correspondence with Globe Tech
2165	Correspondence with Globe Tech
2166	Correspondence with Globe Tech
2167	Correspondence with Globe Tech
2168	Correspondence with Globe Tech
2169	Correspondence with Globe Tech
2170	Correspondence with Globe Tech
2171	Correspondence with Globe Tech
2172	Correspondence with Globe Tech
2173	Correspondence with Globe Tech
2174	Correspondence with Globe Tech
2175	Correspondence with Globe Tech
2176	Correspondence with Globe Tech
2177	Correspondence with Globe Tech
2178	Correspondence with Globe Tech
2179	Correspondence with Globe Tech
2180	Correspondence with Globe Tech
2181	Correspondence with Globe Tech
2182	Correspondence with Globe Tech
2183	Correspondence with Globe Tech

Exhibit Number	Description
2184	Correspondence with Globe Tech
2185	Correspondence with Globe Tech
2186	Correspondence with Globe Tech
2187	Correspondence with Globe Tech
2188	Correspondence with Globe Tech
2189	Correspondence with C. Tsai
2190	Correspondence with Globe Tech
2191	Correspondence with Globe Tech
2192	Correspondence with Globe Tech
2193	Correspondence with Globe Tech
2194	Correspondence with Globe Tech
2195	Correspondence with Globe Tech
2196	Correspondence with Globe Tech
2197	Correspondence with Globe Tech
2198	Correspondence with J. Ong
2199	Correspondence with C. Tsai
2200	Correspondence with J. Ong
2201	Cisco Switch Feature Support Matrix
2202	Correspondence with M. Banin
2203	Correspondence with A. Lee
2204	Correspondence with M. Banin
2205	Correspondence with M. Banin
2206	Correspondence with M. Banin
2207	Correspondence with M. Banin
2208	Correspondence with M. Banin
2209	Correspondence with M. Banin
2210	Correspondence with M. Banin
2211	Correspondence with patent counsel
2212	Correspondence with patent counsel
2213	Correspondence with patent counsel
2214	Correspondence with patent counsel
2215	Correspondence with patent counsel
2216	Correspondence with patent counsel
2217	Correspondence with patent counsel
2218	Correspondence with patent counsel
2219	Correspondence with patent counsel
2220	Correspondence with patent counsel

Exhibit Number	Description
2221	Correspondence with patent counsel
2222	Correspondence with patent counsel
2223	Correspondence with patent counsel
2224	Correspondence with patent counsel
2225	Correspondence with patent counsel
2226	Correspondence with patent counsel
2227	Correspondence with patent counsel
2228	Correspondence with patent counsel
2229	Correspondence with patent counsel
2230	Correspondence with patent counsel
2231	Correspondence with patent counsel
2232	Correspondence with patent counsel
2233	Correspondence with patent counsel
2234	Correspondence with patent counsel
2235	Correspondence with patent counsel
2236	Correspondence with patent counsel
2237	Correspondence with patent counsel
2238	Correspondence with patent counsel
2239	Correspondence with patent counsel
2240	Correspondence with patent counsel
2241	Correspondence with patent counsel
2242	Correspondence with patent counsel
2243	Correspondence with patent counsel
2244	Correspondence with patent counsel
2245	Correspondence with patent counsel
2246	Correspondence with patent counsel
2247	Correspondence with patent counsel
2248	Correspondence with patent counsel
2249	Correspondence with patent counsel
2250	Correspondence with patent counsel
2251	Correspondence with patent counsel
2252	Correspondence with patent counsel
2253	Correspondence with patent counsel
2254	Correspondence with patent counsel
2255	Correspondence with patent counsel
2256	Correspondence with patent counsel
2257	Correspondence with patent counsel

Exhibit Number	Description
2258	Correspondence with patent counsel
2259	Correspondence with patent counsel
2260	Correspondence between S. Lum and A. Lee
2261	Correspondence between S. Lum and A. Lee
2262	Correspondence with patent counsel
2263	Correspondence with patent counsel
2264	Correspondence with patent counsel
2265	Correspondence with patent counsel
2266	Correspondence with patent counsel
2267	Correspondence with patent counsel
2268	Correspondence with patent counsel
2269	Correspondence with patent counsel
2270	Correspondence with patent counsel
2271	Correspondence with patent counsel
2272	Intentionally Left Blank
2273	Correspondence between S. Lum, J. Ong, C. Tsai and A. Lee
2274	Correspondence between S. Lum, C. Tsai and A. Lee
2275	Internal Notes
2276	Correspondence between C. Tsai, J. Ong and S. Lum
2277	Correspondence between C. Tsai, J. Ong and S. Lum
2278	Correspondence between C. Tsai, J. Ong and S. Lum
2279	Correspondence between C. Tsai, J. Ong and S. Lum
2280	Correspondence between C. Tsai and S. Lum
2281	Correspondence between T. Nakano and S. Lum
2282	Draft Meetinghouse Agreement
2283	Correspondence with Globe Tech
2284	Intentionally Left Blank
2285	Correspondence between S. Lum and corporate counsel
2286	Intentionally Left Blank
2287	Correspondence with Globe Tech
2288	Correspondence with Globe Tech
2289	Correspondence with Globe Tech
2290	Correspondence with Globe Tech
2291	Correspondence with Globe Tech
2292	Correspondence with Globe Tech
2293	Correspondence with Globe Tech
2294	Correspondence with Globe Tech

Exhibit Number	Description
2295	Correspondence with Globe Tech
2296	Correspondence with Globe Tech
2297	Correspondence with Globe Tech
2298	Correspondence between S. Lum and J. Ong
2299	Correspondence between S. Lum and J. Ong
2300	Correspondence with Globe Tech
2301	Correspondence with Globe Tech
2302	Correspondence between M. Banin and S. Lum
2303	Correspondence with Globe Tech
2304	Correspondence with Globe Tech
2305	Correspondence with Globe Tech
2306	Correspondence with Globe Tech
2307	Correspondence with Globe Tech
2308	Correspondence with Globe Tech
2309	Correspondence with Globe Tech
2310	Correspondence with Globe Tech
2311	Correspondence with Globe Tech
2312	Correspondence with Globe Tech
2313	Correspondence with Globe Tech
2314	Correspondence with Globe Tech
2315	Correspondence with Globe Tech
2316	Correspondence with Globe Tech
2317	Correspondence with Globe Tech
2318	Correspondence with Globe Tech
2319	Correspondence with Globe Tech
2320	Correspondence with Globe Tech
2321	Correspondence with Globe Tech
2322	Correspondence with Globe Tech
2323	Correspondence with Globe Tech
2324	Correspondence with Globe Tech
2325	Correspondence with Globe Tech
2326	Correspondence with Globe Tech
2327	Draft Patent Application
2328	Draft Patent Application
2329	CyberGatekeeper Enforcement Modes
2330	CyberGatekeeper Enforcement Modes
2331	Correspondence with Globe Tech

Exhibit Number	Description
2332	Correspondence with Globe Tech
2333	Correspondence with Globe Tech
2334	Correspondence with Globe Tech
2335	Correspondence with Globe Tech
2336	Correspondence with Globe Tech
2337	Correspondence with Globe Tech
2338	Correspondence with Globe Tech
2339	Correspondence with Globe Tech
2340	Internal InfoExpress Correspondence
2341	Intentionally Left Blank
2342	Internal InfoExpress Correspondence
2343	Correspondence with Globe Tech
2344	Correspondence with Globe Tech
2345	Correspondence with Globe Tech
2346	Correspondence with Globe Tech
2347	Correspondence with Globe Tech
2348	Correspondence with Globe Tech
2349	Correspondence with Globe Tech
2350	Correspondence with Globe Tech
2351	Correspondence with Globe Tech
2352	Correspondence with Globe Tech
2353	Correspondence with Globe Tech
2354	Correspondence with Globe Tech
2355	Correspondence with Globe Tech
2356	Correspondence with Globe Tech
2357	Correspondence with Globe Tech
2358	Correspondence with Globe Tech
2359	Correspondence with Globe Tech
2360	Correspondence with Globe Tech
2361	Correspondence with Globe Tech
2362	Correspondence with Globe Tech
2363	Correspondence with Globe Tech
2364	Correspondence with Globe Tech
2365	Correspondence with Globe Tech
2366	Correspondence with Globe Tech
2367	Correspondence with Globe Tech
2368	Correspondence with Globe Tech

Exhibit Number	Description
2369	Correspondence with Globe Tech
2370	Correspondence with Globe Tech
2371	Correspondence with Globe Tech
2372	Correspondence with Globe Tech
2373	Correspondence with Globe Tech
2374	Correspondence with Globe Tech
2375	Correspondence with Globe Tech
2376	Correspondence with Globe Tech
2377	Correspondence with Globe Tech
2378	Correspondence with Globe Tech
2379	Correspondence with Globe Tech
2380	Correspondence with Globe Tech
2381	Correspondence with Globe Tech
2382	Correspondence with Globe Tech
2383	Intentionally left blank
2384	Correspondence with Globe Tech
2385	Correspondence with Globe Tech
2386	Internal InfoExpress Correspondence
2387	Correspondence with Globe Tech
2388	Correspondence with Globe Tech
2389	Internal InfoExpress Correspondence
2390	Correspondence with Globe Tech
2391	Intentionally left blank
2392	Intentionally left blank
2393	Intentionally left blank
2394	Intentionally left blank
2395	Correspondence with Globe Tech
2396	Internal InfoExpress Correspondence
2397	Correspondence with Globe Tech
2398	Intentionally left blank
2399	Correspondence with Globe Tech
2400	Correspondence with Globe Tech
2401	Correspondence with Globe Tech
2402	Correspondence with Globe Tech
2403	Correspondence with Globe Tech
2404	Correspondence with Globe Tech
2405	Correspondence with Globe Tech

Exhibit Number	Description
2406	Correspondence with Globe Tech
2407	Correspondence with Globe Tech
2408	Correspondence with Globe Tech
2409	Correspondence with Globe Tech
2410	Correspondence with Globe Tech
2411	Tim Greene, InfoExpress Simplifies Security Devices, NetworkWorld (Dec. 6, 2004), available at https://www.networkworld.com/article/875004/lan-waninfoexpress-simplifies-security-devices.html
2412	InfoExpress's Objections and Responses to Cisco's First Set of Interrogatories (Nos. 1-12), served in InfoExpress Inc. v. Cisco Systems, Inc., Case No. 4:23-cv-2698-YGR (N.D. Cal.).
2413	Cisco Systems, Inc., Network Admission Control White Paper (2004).
2414	Correspondence with Cisco
2415	Email attachment to EX2414
2416	Correspondence with Cisco
2417	Email attachment to EX2416
2418	Correspondence with Cisco
2419	Correspondence with Cisco
2420	Correspondence with Cisco and KeyLabs
2421	Email attachment to EX2420
2422	Correspondence with Cisco
2423	Correspondence with Cisco
2424	Email Attachment to EX2423
2425	Intentionally Left Blank
2426	Intentionally Left Blank
2427	Declaration of Aaron R. Striegel, PhD
2428	Intentionally Left Blank
2429	Declaration of Yuhshiw Alice Lee
2430	LAN Based Policy Enforcement Engineering Specification
2431	Metadata for EX2430
2432	LAN Based Policy Enforcement Engineering Specification
2433	Metadata for EX2432
2434	Internal InfoExpress Correspondence
2435	Internal InfoExpress Correspondence
2436	Additional Metadata for EX2011

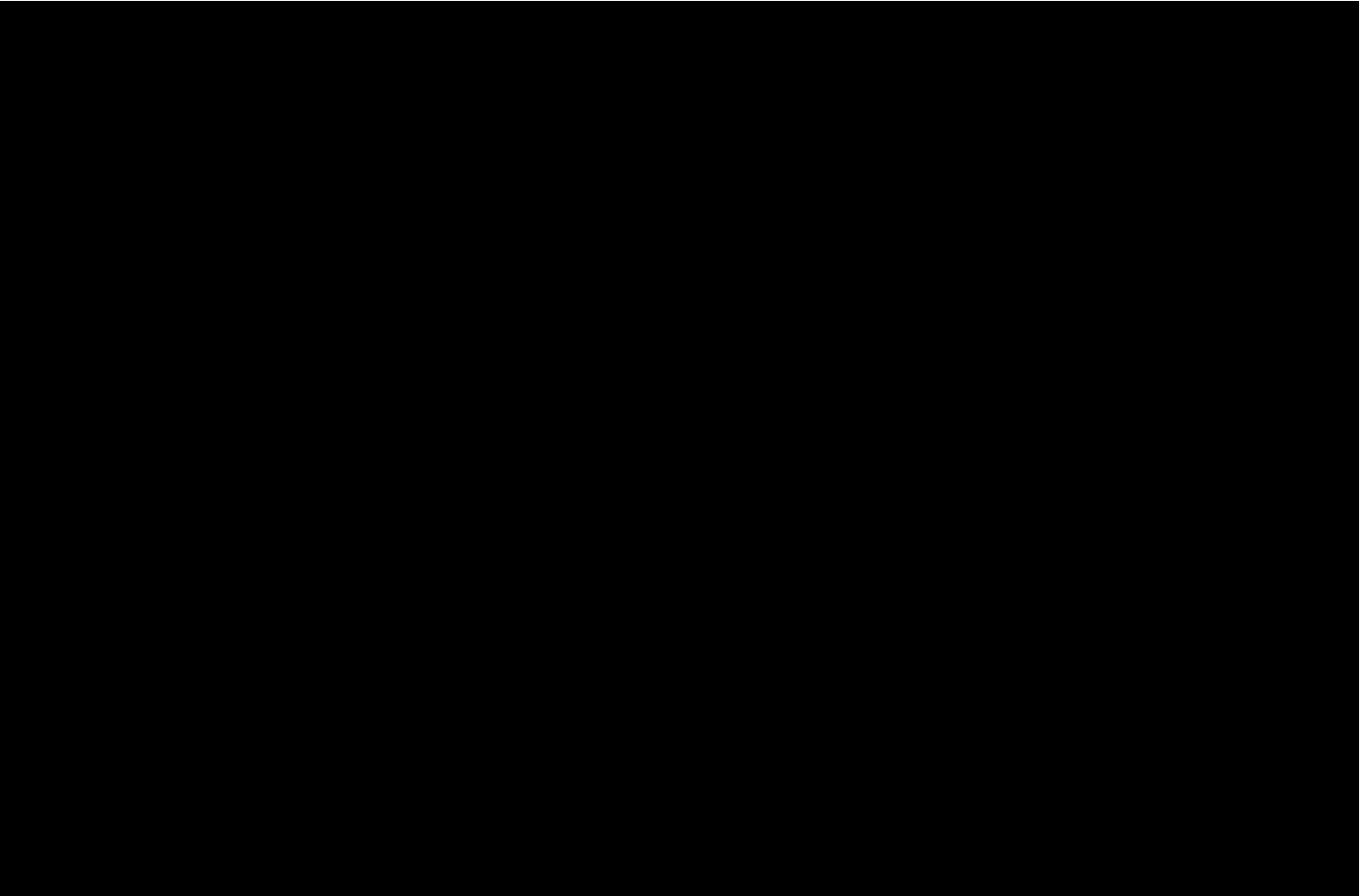
Exhibit Number	Description
2437	LAN Based Policy Enforcement Engineering Specification
2438	Metadata for EX2437
2439	Internal InfoExpress Correspondence
2440	Internal InfoExpress Correspondence
2441	Internal InfoExpress Correspondence
2442	Internal InfoExpress Correspondence
2443	Design Specifications
2444	Design Specifications
2445	RADIUS Protocol Spoofing Vulnerability (Blast-RADIUS) July 2024
2446	Tim Greene, Deceiving Ciscos NAC (April 3, 2007)
2447	Hasham Ud-Din Qazi, Comparative Study of Network Access Control Technologies
2448	Thumann and Rocher, Hacking the Cisco NAC Framework Blackhat USA 2007 Whitepaper
2449	Deposition of Henry Houh, December 4, 2024
2450	Dkt 121 – Claim Construction Order dated September 25, 2024 [InfoExpress, Inc. v, Cisco Systems, Inc. [4:23-cv-02698-YGR]
2451	Mobile Agent Deployment Guide
2452	Reference Manual
2453	Server User’s Guide
2454	CGX 2.3 – Standalone Guide
2455	CGX 2.2 Complete Guide
2456	CGX Appliance Specifications
2457	Solutions Guide
2458	Intentionally Left Blank
2459	CGX Access Deployment Guide
2460	Installation Guide v9.0
2461	About CGX
2462	CGX 1.0 Frequently Asked Questions
2463	CGX Access - Frequently Asked Questions
2464	CGX Access Guide
2465	Solutions Guide
2466	CGX 2.2 Complete Guide
2467	Solutions Guide
2468	Installing CGX
2469	Correspondence with Scotia Bank

Exhibit Number	Description
2470	Correspondence with Cisco
2471	Internal InfoExpress Correspondence
2472	Cisco Announces Continued Momentum within Network Admission Control Industry Initiative
2473	Correspondence with Cisco
2474	Correspondence with Cisco
2475	Cisco NAC and CyberGatekeeper Technical White Paper
2476	Internal Cisco Correspondence
2477	Correspondence with Cisco
2478	LAN Technology Presentation
2479	Correspondence with Cisco
2480	NAC Overview
2481	Correspondence with Cisco
2482	Correspondence with Cisco
2483	Partner Solution Brief – NAC Deployment
2484	Cisco NAC + CyberGatekeeper vs. Competitive Enforcement Solutions
2485	Correspondence Between Cisco, InfoExpress and Burton Group
2486	RSA Conference 2005 Slide Deck
2487	Internal InfoExpress Correspondence
2488	RSA Conference 2005 Slide Deck
2489	Correspondence with Cisco
2490	Cisco NAC + CyberGatekeeper vs. Competitive Enforcement Solutions
2491	Partner Solution Brief – NAC Deployment
2492	Correspondence with Cisco
2493	Internal InfoExpress Correspondence
2494	NAC IVT Test Plan/Report
2495	Correspondence with Cisco
2496	Correspondence with Cisco
2497	Virtual Machine Preparation for Cisco
2498	Internal InfoExpress Correspondence
2499	Virtual Machine Preparation for Cisco
2500	InfoExpress NAC Demo
2501	Internal InfoExpress Correspondence
2502	Protected Network, ScienceDirect Topics
2503	Correspondence with Cisco

Exhibit Number	Description
2504	Introduction to CyberGatekeeper
2505	Correspondence with Cisco
2506	Correspondence with Cisco
2507	Correspondence with Cisco
2508	Correspondence with Cisco
2509	Correspondence with Cisco
2510	Internal Cisco Correspondence
2511	Correspondence with Cisco
2512	Internal Cisco Correspondence
2513	Correspondence with Cisco
2514	Internal InfoExpress Correspondence
2515	Internal Cisco Correspondence
2516	Correspondence with Cisco
2517	Correspondence with Cisco
2518	Intentionally Left Blank
2519	NAC2 Beta Deployment Guide
2520	Internal InfoExpress Correspondence
2521	U.S. Patent No. 5,987,611
2522	Request for Comment: 2865
2523	Internal InfoExpress Correspondence
2524	Winning with CyberGatekeeper from InfoExpress
2525	Tim Greene, Burning NAC questions – Part 2, Network World (Oct 17, 2007)
2526	Paul Roberts, Black Hat: NAC Solutions Vulnerable to Attack, ComputerWorld (Aug 3, 2006)
2527	Correspondence with Cisco
2528	Memorandum re: Product Announcement
2529	LAN Technology PowerPoint
2530	Posture Plugin Development
2531	Product Guidelines
2532	Technical File Information
2533	Project File
2534	Project File
2535	Project File
2536	Project File
2537	Project File
2538	Project File

Exhibit Number	Description
2539	Project File
2540	Project File
2541	Technology Overview
2542	Policy Manager Reference Manual
2543	CGS Reference Manual
2544	LAN Enforcement Module Reference Manual
2545	EAP Enforcement Module Reference Manual
2546	8021X Authentication Procedures
2547	Internal InfoExpress Correspondence
2548	Correspondence with Cisco
2549	Cisco Release Notes
2550	Cisco Trust Agent Administrator Guide
2551	Internal InfoExpress Correspondence
2552	NAC AVP Specification
2553	NAC Architecture Overview
2554	HCAP
2555	Correspondence with GTI
2556	Engineering Specifications
2557	LAN Based Policy Enforcement Components
2558	LAN Based Policy Enforcement Engineering Specifications
2559	LAN Based Policy Enforcement Engineering Specifications
2560	LAN Based Policy Enforcement Components
2561	LAN Based Policy Enforcement Engineering Specifications
2562	LAN Based Policy Enforcement Engineering Specifications
2563	LAN Based Policy Enforcement Components
2564	Supplemental Declaration of Stacey Lum
2565	Supplemental Declaration of Dr. Eric Cole
2566	Tanenbaum Excerpts
2567	IEEE 802.1 1x (2001)
2568	InfoExpress's Objections and Responses to Cisco's Second Set of Interrogatories (4/11/2024)
2569	Heartbeat (computing) Semantic Scholar

I. INTRODUCTION



II. PETITIONER'S UNPATENTABILITY GROUNDS

Petitioner raises one ground asserting the Challenged Claims are obvious in view of ("Krantz") (EX1205) in view of ("Herrmann") (EX1206).

III. THE 444 PATENT

A. Date of Invention

Patent Owner submits for the reasons discussed in section 0 the date of invention for each of the Challenged Claims is no later than December 2, 2002.

B. POSITA

Petitioner's and Patent Owner's POSITA contentions are similar. Petitioner contends a POSITA "would have had a bachelor's degree in computer science, computer engineering, or an equivalent, and two years of relevant experience in networking and network security, and related fields." Pet. at 4. Patent Owner agrees on the educational background, and contends that "at least three years of experience in networking operating systems and cybersecurity" or "a master's degree in one of the foregoing and at least two years of experience..." is appropriate. Patent Owner does not contend this difference affects the outcome.

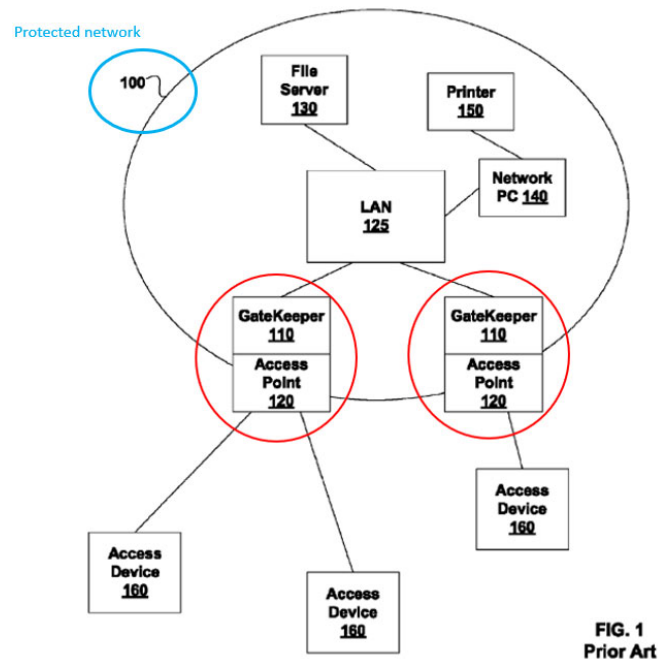
C. Overview of the 444 Patent

The Patent is directed to a seminal approach to addressing computer network security concerns and controlling access to a protected network while overcoming shortcomings in the prior art with scalability and slowed network traffic. Before Patent Owner's inventions, network security required multiple "gatekeepers" placed directly between clients (*i.e.*, users) and the protected network, *i.e.*, inline. EX1201, Fig. 1, 2:34-45; EX2001, ¶¶44-46.

The patent explains prior-art network control approaches included providing systems outside of or at the periphery of a protected network for authenticating a user or device, such as by checking user ID and password or MAC address. *Id.*, 1:39-42. The patent then explains reliance on authentication alone suffers from

disadvantages including not assuring the device meets security policies, such as out-of-date virus software. *Id.*, 1:51-55.

The patent describes as "prior art" the following architecture.



EX1201, Fig. 1 (annotated). The protected network 100 included multiple access points, each including a Gatekeeper 110 where one or more access devices attempting to connect to the protected network must pass through an access point and its gatekeeper. The Patent explains that the "use of one instance of GateKeeper 110 to support numerous instances of Access Device 160 is limited by bandwidth and required sophistication (e.g., cost) of GateKeeper 110." EX1201, 2:35-38. The inline gatekeeper also becomes a limiting bottleneck on the bandwidth of the system. EX1201, 2:39-42.

The Patent addressed these scalability and bandwidth shortcomings with architecture locating a gatekeeper on a subset of the protected network itself, and by providing for configuring an access point so previously authorized devices can access the network without tying up bandwidth and as many computer resources.

The Patent discloses a protected network 200 including a restricted subset 205 with a gatekeeper 225 thereon, and one or more less-restricted subsets 210 of the protected network with other network resources.

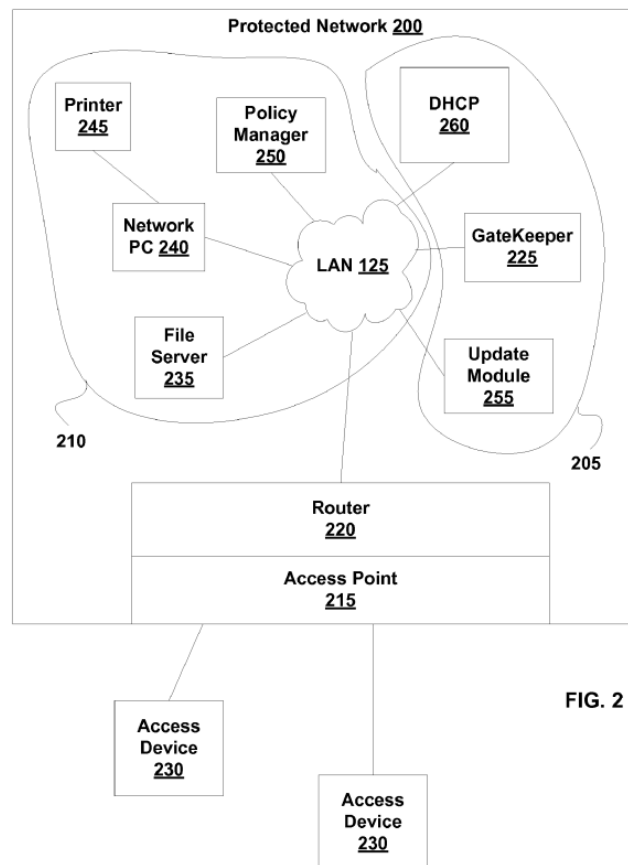


FIG. 2

EX1201, Fig. 2, 5:58-7:59. Before an access device is granted access to the less-restricted subset 210, its request is passed to the restricted subset 205. EX1201, 5:36-

57. A gatekeeper in the restricted subset evaluates whether the access device satisfies security policies, and if so, the access device may access a less-restricted subset of the protected network. EX1201, 2:48-53.

The Patent further describes access device auditing to determine security policy compliance. . EX1201, 6:42-49. If the device configuration satisfies access-device security policy requirements, it may be granted access to the restricted subset of the protected network. EX1201, 2:58-60.

Another claimed feature of the Patent is the configuring of the access point after user authentication and access-device compliance with a security policy are determined. EX1201, Claims 2 & 22. The Patent explains "reconfiguration typically includes reassigning the communication port from the restricted VLAN to the less-restricted VLAN." *Id.*, 3:22-25.¹

¹ While the "typical" embodiment discussed utilizes VLANs, the 444 Patent further explains other access point embodiments may be utilized, including "wireless access point and MAC addresses, or the like, are used instead of VLANs to separate traffic from different instances of Access Device 230." *Id.*, 15:25-30.

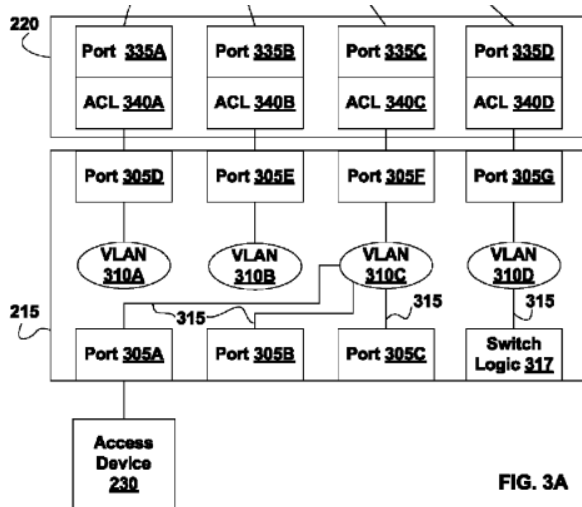


FIG. 3A

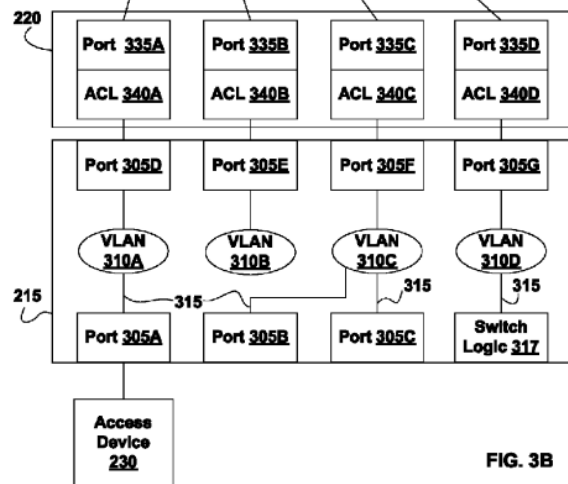


FIG. 3B

Switch Logic 317 is configured for configuring and reconfiguring members of Ports 305A-305G responsive to received commands. For example, by receiving an appropriate command, Switch Logic 317 is configured to reconfigure Port 305A to be associated with VLAN 310A, as illustrated in FIG. 3B below. In this configuration, data received at Port 305A is directed to Port 305D via VLAN 310A, rather than to Port 305F. EX1201, 8:25-32.

As known at the time of the invention, when setting up a network, access points must be configured. Cole Decl. (EX2565), ¶56. This can include configuring communication port VLAN assignments, establishing access control lists (ACL), or other configurations by the network administrator. *See, e.g.*, EX1201, 13:10-28.

By changing the configuration of communication port assignments or ACL after authenticating and auditing an access device, *i.e.*, configuring the access point after the initial configuration setup, data from authorized devices can pass to the less-restricted subset of the protected network without first passing through the

gatekeeper on the restricted subset of the protected network. Thus, the prior art shortcomings are avoided.

In other embodiments, the Patent describes additional advantages from continuing audits of the access device for compliance with a security policy even after it is granted permission to access the less-restricted subset of the protected network. EX1201, 13:64-14:11.

IV. THE CITED ART

Petitioner's art is not prior art. Even if so, the references are distinctly different from the patent.

A. Krantz

Krantz relates to "provisioning" and accessing the Internet via an Internet Service Provider (ISP). EX1205, [0005] ("before a computer system can communicate electronically on the Internet, a user of the computer system is often required to register with an Internet Service Provider ... that can authorize access to the Internet."). Popular ISPs at that time included America Online (AOL).

Krantz describes the basic concept for accessing virtually any network: "[a] user must first send 'credentials' to the server, which can be a 'Remote Authentication

Dial-In User Service ('RADIUS') server."² *Id.* Such credentials being "user identifier and password." *Id.*, [0076].

Krantz's purported enhancement relates not to network security but to "automation when ***provisioning*** a computer system" (EX1205, title). In the late-1990's, "users wishing to access the Internet are subjected to contacting an ISP telephonically and waiting for appropriate access software and/or hardware to be delivered." *Id.*, [0008]. Krantz explains "many [ISP] services are proprietary and each service may require different computer system configurations and/or registration information for authorizing access to the Internet" *Id.*, [0011]. To provision a user's device with ISP software, Krantz downloads "provisioning files," rather than waiting for ISP software in the mail. *Id.*, [0032], [0085].

Dodging Krantz's "provisioning" *raison d'etre*, Petitioners focus on an aspect of Krantz explaining how the user's data, after the user is authorized, is directed to the Internet through VLANs.

[A]ccess to resources located on network 413 can be restricted by the use of Virtual Local Area Networks ("VLANs"). In these embodiments, ***networks 411, 412 and 413*** may each be a portion of a different VLAN. ***VLAN aware devices in network architecture 400 can "Tag" data frames*** to indicate to data routing device 414 where the data frames are

² RADIUS is a networking protocol providing centralized authentication for users who connect and use a network service. RADIUS was later brought into IEEE 802 standards. <https://en.wikipedia.org/wiki/RADIUS>.

to be routed. For example, when client 405 is not authorized to access resources located network 413, components in network 411 or logical communication link 433 can ***Tag data frames from client 405*** indicating that the data frames are to be routed to server 415 (or other resources located on network 412). When client 405 is authorized to access network 413, components in network 411 or logical communication link 433 can ***Tag data frames from client 405*** indicating that the data frames are to be routed to resources on network 413 (e.g., to the Internet) or to resources on network 412 (e.g., server 412) as appropriate.

Id., [0052].

Krantz teaches nothing about device security compliance or about configuring an access point after user authentication. Instead, Krantz teaches the VLAN-aware access point relabels ***client*** data routing information and the client data is routed according to access point's configuration. EX2565, ¶62. Krantz does not disclose configuring the access point itself as part of applying a security policy. *Id.*, ¶¶73-82, 57-58, 62-64.

B. Herrmann

Herrmann discloses a system for security policy enforcement before allowing a client device access to a protected network. Like the prior art discussed by the Patent, Herrmann teaches an access point, a Network Access Server (NAS) positioned outside of a protected network and between a client device and protected network resources. *See* Fig. 4.

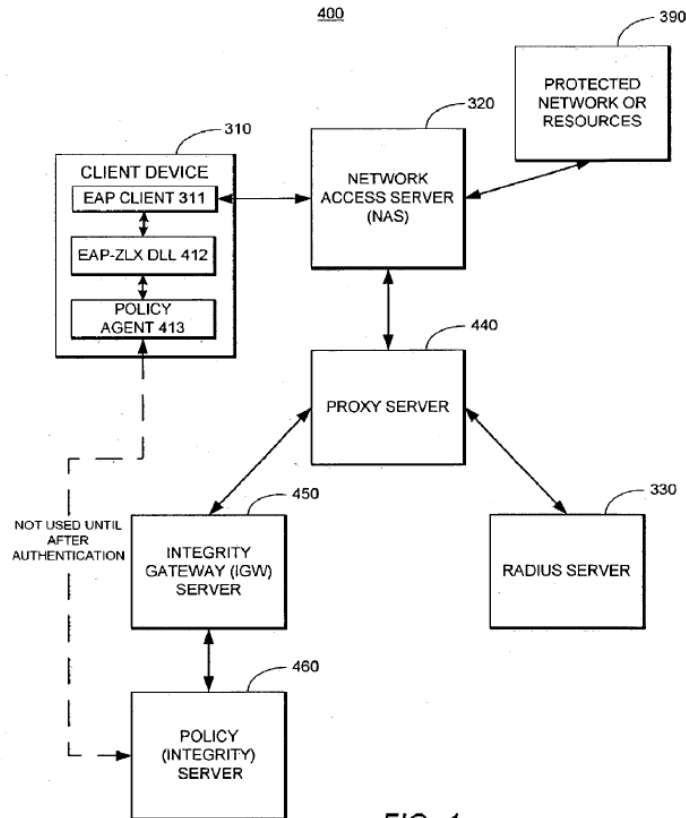


FIG. 4

Referring to Fig. 4, Herrmann explains a client device must first pass a Network Access Server (NAS) to access a protected network. EX1206, [0063]. The NAS then, through a Proxy Server, authenticates the user with a Radius Server. EX1206, [0073-0076]. After authenticating user identity, an agent on the client gathers information about it, which is then communicated to the NAS, then the Proxy Server, and then the Integrity Gateway Server (IGW). EX1206, [0074, 0077-0079]. The IGW then formats and packages the data for transmission to the Policy (Integrity) Server. EX1206, [0096]. This Policy (Integrity) Server then unpacks the data and determines if the client device includes anti-virus software. EX1206, [0068]; EX2565, ¶66

All requests from a client to access the protected network must first pass through the NAS, the authentication server, and the policy server before the client is permitted to access the protected network. EX2565, ¶67. After the session is approved, Herrmann discloses nothing regarding additional monitoring of the client device during the session or modifications to the system components in view of the approval process. *Id.*, ¶68.

V. CLAIM CONSTRUCTION

The "words of a claim 'are given their ordinary and customary meaning,'" which "is the meaning that the term would have to a person of ordinary skill in the art in question at the time of the invention." *Phillips v. AWH Corp.*, 415 F.3d 1303, 1313 (Fed. Cir. 2005) (en banc). The Board must construe disputed terms to the extent necessary to resolve the controversy. *Realtime Data, LLC v. Iancu*, 912 F.3d 1368, 1375 (Fed. Cir. 2019).

Petitioner offers no construction for any claim term, and instead contends under any claim construction the asserted art discloses each claimed limitation. Petition at 7. Petitioner conflates claim construction with patentability, which is improper. *Amazon. com, Inc. v. Barnesandnoble. com, Inc.*, 239 F. 3d 1343, 1351 (Fed. Cir. 2001) ("[T]he first step of an invalidity analysis ... in view of prior art references is no different from that of an infringement analysis. ... [T]he first step is to determine the meaning and scope of each claim in suit.") (quotation omitted).

"Configuring the Access Point"

Claims 2-7 and 22 include the limitation "configuring the access point." This configuring of the access point is part of the step "applying the security policy." It appears the Board implicitly gave some meaning to the scope of this claim term by determining there to be a sufficient showing of "applying the security policy includes configuring the access point" by a "VLAN aware device [that] can insert Tag Headers into data frames received from [the] client" ID at 29. Such an implicit claim construction is incorrect.

The plain meaning for "configuring the access point" as part of the application of the security policy requires there to be a change to the access point's initial configuration after applying the security policy. This is readily apparent from a reading of the overall claim. Claim 1 specifies that prior to applying the security policy the access point is "configured to use an 802.1x protocol." EX1201, Claim 1. The gatekeeper then applies a security policy to the audit data. *Id.* Thus, "applying the security policy" involves application of a security policy to an already configured access point, *e.g.*, its initial configuration. This same analysis applies to claim 22. EX1201, Claim 22.

Logically, "configuring the access point" as part of applying a security policy means changing the configuration of the previously configured access point.

Importantly, the claims specify the access point itself is configured, not that the access point configures something else.

“A Method For Auditing A Device”

The preamble of claims 1 and 22 recites a "method for auditing a device" and should be construed as limiting. "Whether to treat a preamble as a limitation is a determination 'resolved only on review of the entire[] ... patent to gain an understanding of what the inventors actually invented and intended to encompass by the claim.'" *Shoes By Firebug v. Stride Rite Children's Group*, 962 F.3d 1362, 1367 (Fed. Cir. 2020) (quotations omitted). "[A] preamble limits the invention if it recites essential structure or steps, or if it is necessary to give life, meaning, and vitality to the claim." *Id.* (quotations omitted). While there is no precise test for when a preamble limits claim scope, "dependence on a particular disputed preamble phrase for antecedent basis may limit claim scope because it indicates a reliance on both the preamble and claim body to define the claimed invention." *Id.* (quotations omitted).

The Petition treats the claim as limiting and makes no suggest that it is not. Pet. at 20-22. Indeed, the preamble sets the stage and provides antecedent basis for what is being audited, namely, a "device:" EX1201, 16:9-12 and 17:10-13 ("A method for auditing a device..." and "the device."). The Federal Circuit has explained that "use of preamble terms to define positive limitations in the body of

claims can evince an inventor's intent that the preamble limit the scope of the claim.”
See Shoes By Firebug, 962 F.3d at 1368.

Here, the preamble defines what the claimed methods “do”, namely, "auditing a device." *See, e.g., Boehringer Ingelheim Vetmedica, Inc. v. Schering-Plough Corp.*, 320 F.3d 1339, 1345 (Fed.Cir. 2003) (“In contrast to apparatus and composition claims, claims to methods of using such apparatuses or compositions are not directed to what the method ‘is,’ but rather they typically rely entirely on what the method ‘does.’ And what a method does is usually recited in its preamble. Accordingly, our claim construction analysis of statements of intended purpose in methods of using apparatuses or compositions has tended to result in a conclusion that such preamble language is limiting.”); *Bell Communications Research, Inc. v. Vitalink Communications Corp.*, 55 F.3d 615, 620 (Fed.Cir. 1995) (“[W]hen the claim drafter chooses to use both the preamble and the body to define the subject matter of the claimed invention, the invention so defined, and not some other, is the one the patent protects.”). Indeed, the body of claims 1 and 22 say the same requiring: "receiving ***audit data ... pertaining to the device***" and "applying a security policy that includes at least ***one requirement pertaining to the audit data*** and at least one requirement pertaining to the authentication." EX1201, 16:16-21 and 17:15-25.

Accordingly, the preamble should be construed as limiting.

VI. KRANTZ AND HERRMANN FAIL TO RENDER THE CHALLENGED CLAIMS OBVIOUS

A. Krantz Does Not Disclose "A Method For Auditing A Device" or "Audit Data"

The preamble of claims 1 and 22 recite a "method for auditing a device." The Challenged Claims also recite various "audit data" limitations. Krantz discloses neither. Notwithstanding, Petitioner relies on Krantz alone for purportedly disclosing the preamble. Pet. at 20-24 and 86. Krantz only discloses user authentication; not device auditing. "Auditing" is explained in the Patent as being directed to ensuring the **device** attempting to access the protected network to complies with the security policy requirements.

The specification further distinguishes user authentication and device auditing: prohibiting network access "until authentication with the authentication server passes AND an audit with the software agent... passes." EX1201, 14:4-14. Also, FIG. 4 shows "authenticate user 440," "obtain audit data 450," and "apply security policy 460" are all different steps.

GateKeeper 225 authenticates a user, obtains audit data, and applies a security policy in an Authenticate User Step 440, an Obtain Audit Data Step 450 and an Apply Security Policy Step 460, respectively.

EX1201, 10:43-45.

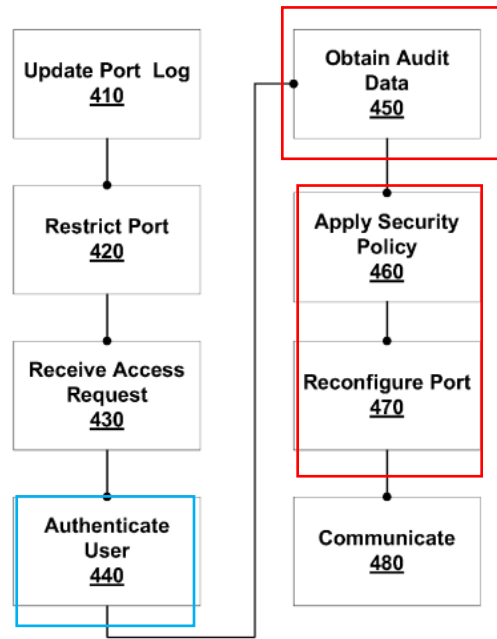


FIG. 4

Petitioner repeatedly mixes, matches, and conflates user authentication and auditing/audit data. Here, Petitioner’ asserts Krantz’s “user-identifier[s] and password[s]” are both “audit data” and “authentication.”

message that can be transferred through the access point.” Ex.1205, [0018]. Other “**audit data**” provided by Krantz’s “*device*” may include, for example, “user-identifier[s] and password[s].” Ex.1205, [0076]. Krantz further explains that

Pet. at 21

Krantz discloses:

When credentials are sent to server 215, authentication module 217 can receive the credentials (e.g., **user-identifier and password**) and compare the credentials [*“apply[ing] a security policy”*] to entries in **user database** 218. If credential information matches ... **the identity of a user is authenticated** (server 215 believes that the user represented by the user-identifier is the user who entered the credential information) [*“that includes at least on requirement pertaining to authentication”*]. If an

Pet. at 59

In actuality, Krantz only discloses **user** authentication data. Not **device** "audit data" and **device** "auditing." Petitioner even admits this.

- "Krantz explains that ... '**authentication module 217** can receive the credentials (e.g. user-identifier and password) and compare the credentials to entries in the user database 218.'" Pet. at 55.
- "If an **authenticated user** of the client 205 is authorized to access resources..." *Id.*
- "Krantz explains that the ‘method 300 includes act of [client 205] sending credentials to a server to attempt to **authenticate** with the server...' *Id.* at 28-29.
- "A presented user-interface can be used to receive user-entered information (e.g., user-identifier, password, name, address, credit card information, etc.) from a user at client 205." *Id.* at 40-41.

In fact, this Board provided helpful context in other related institution denials demonstrating the differences between Krantz's authentication-only approach and the auditing a security policy on the access device:

"Thus, Petitioner has not shown sufficiently that Krantz teaches the step of auditing the device in accordance with a security policy." IPR2025-0549, Paper 13 (Inst. Denial) at 14.

"The '350 patent distinguishes between user authentication using a username and password and application of a security policy." *Id.* at 12.

"Although the '350 patent describes both user authentication and application of a security policy as being carried out by a gatekeeper, this is accomplished in separate process steps... . user authentication and application of a security policy are separate processes." *Id.* at 12-13.

"As such, Petitioner relies on essentially the same analysis based on Krantz for teaching two processes that are expressly distinguished in the specification of the '645 patent. Because Petitioner fails to develop a coherent unpatentability theory with respect to both the 'audit' and 'authentication' limitations, we find that Petitioner has not shown sufficiently that Krantz teaches or suggests 'a gatekeeper... to: formulate an audit request." IPR2024-00678, Paper 14 (Inst. Denial) at 15.

Accordingly, Krantz's *user* authentication disclosures do not pass muster. Since the Petition only relies on Krantz for the preamble, the Ground for unpatentability fails.

B. Krantz Does Not Disclose "Configuring The Access Point"

Each of claims 2-7 and 22 require "configuring the access point"—not configuring something else or that the access point configures something. Petitioner relies on Krantz's disclosure of access point 209 as a VLAN-aware device that can insert Tag Headers into data frames received from client 205 such that the data is transferred to VLAN B and/or VLAN C. Pet. at 63. Krantz does not disclose what is

claimed. Krantz only discloses the access point may configure client data by inserting a Tag Header into the device's data so it is directed according to the access point's predetermined configuration. While this may be reconfiguration or configuration of client data, it is not configuration of the access point.

The issue is not about what component inserts Tag Headers. Rather, inserting Tag Headers into a data frame for data received from an access device is not configuring of the access point at all, and instead is configuring the routing information in the client data. That Krantz's access point may insert the Tag Header does not mean the access point is configured. EX2565, ¶¶79-81. There is no evidence of any *change* to the access point, which instead, merely performs according to its already configured initial settings. *Id.*

As background, when establishing a switched network with VLAN-aware devices, the VLAN devices must first be configured. *See* EX2565, ¶76. To enable a network device to identify frames of different VLANs, a tag field is inserted into the data link layer encapsulation. *Id.* The format of VLAN-tagged frames is defined in the IEEE 802.1Q standard. *Id.* A network device handles an incoming frame depending on whether the frame is VLAN-tagged, and information about the VLAN tags, if any. *Id.*

In Krantz, after a user is authenticated (user ID and password), data fields from the user's device are tagged to allow access to the Internet. The access point

itself is not changed. Rather, data with a particular VLAN ID is directed to the preprogrammed VLAN based on this new tag. EX2566.

When a data frame from a device is received, the VLAN-aware device checks to see if its VLAN tag is in the VLAN database. If it is, the data is sent to the assigned VLAN, which in Krantz is VLAN C. If the VLAN does not have a tag, the data frame is sent to where the access point is configured, i.e., pre-programmed, to send untagged data. In Krantz, the data goes to VLAN B. If server 215 determines that data frame is from an authorized user (user ID and password) then the access point, according to its predetermined configuration, inserts a different Tag Header into the data frame to reroute data to VLAN C. Essentially, when the RADIUS server notifies the access point that the user is authorized, the access point changes the label on the data per its preconfigured programming. EX2565, ¶¶79-80.

Notably, Krantz's access point's configuration is not changed. *Id.*, ¶80. If one argues Krantz's "access point 209" is the claimed "access point," the association of ports 251 and 252 remain unchanged. *Id.* Even if one considers data routing device 214 to be the claimed "access point," there is still no change to the port associations or other setting of the access point. *Id.* Instead, data bearing a Tag Header assigned to VLAN B or untagged will go to VLAN B, and data bearing a Tag Header assigned to VLAN C will go to VLAN C, just as was the case before the client data was

authorized. It is the data frame itself that is changed, not the access point settings.
Id.

It was well-understood to POSITA that configuration of the access point could be done by changing what it does with untagged client data. For example, rather than being sent to a RADIUS server for user authentication, the access point could be reprogrammed so that incoming data without a tag header are dropped. *Id.*, ¶81. While Krantz teaches changing a data frame's label (tag header), the Challenged Claims require something different, namely, changing the configuration of the access point. *Id.*, ¶¶81-82. This is missing entirely from Krantz.

As a fallback, Petitioner argues it would have been obvious to combine access point 209 and data routing device 214. Nonetheless, the same Tag Header argument is made for this hindsight combination of devices. For the reasons discussed, the insertion of tag headers is not configuring the access point.

Further, arbitrarily combining these distinct components finds no support in Krantz. Petitioner's own cited portions of Krantz expressly teach access point 209 and a different component data routing device 214. EX1205, [0073] ("[A]ccess point 209 and/or data routing device 214 may strip the 802.1X encapsulation and instead encapsulate the EAP-Response/Identity messages within an EAP-RADIUS message that is transferred onto VLAN B."). Krantz's teaching confirms any

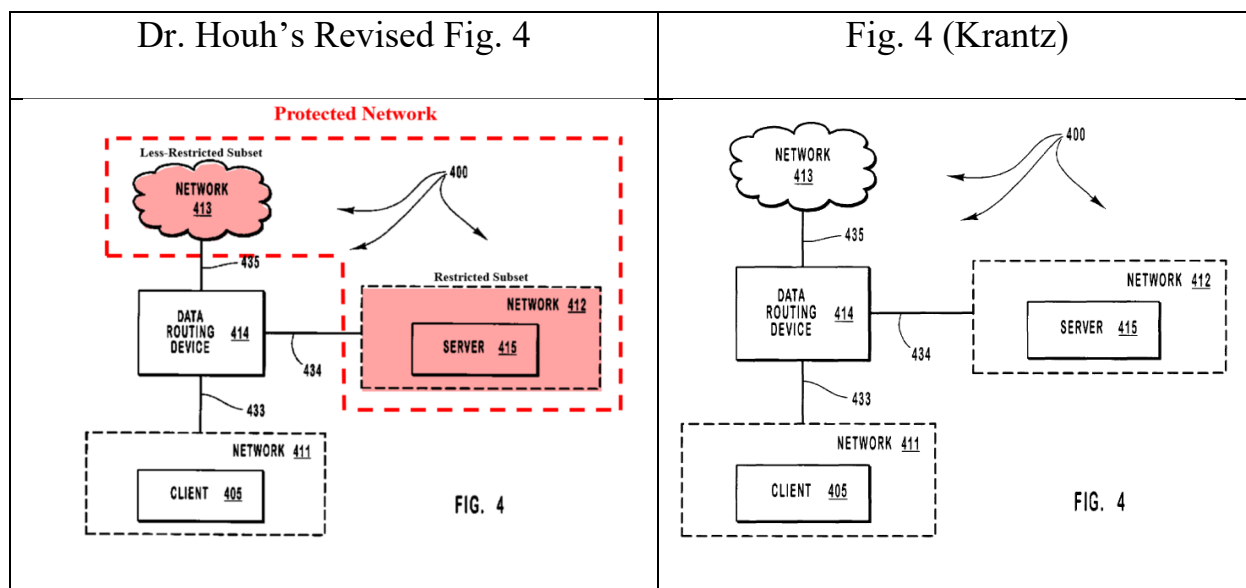
reconfiguration is of user identification data, not an access point as claimed, because "EAP-Response/Identity messages" expressly relate to user authentication.³

C. **Krantz Does Not Disclose A Less-Restricted Subset Of A Protected Network**

Claim 22 recites "a less-restricted subset of the network." The designation of a less-restricted subset of a network, and the implicit restricted subset of the network is explained as providing for a solution to inline gatekeepers that resulted in network bottlenecks and limited scalability. EX1201, Fig. 1, 2:48-58. By establishing "subsets" to the network, bottlenecks and limited scalability issues are ameliorated.

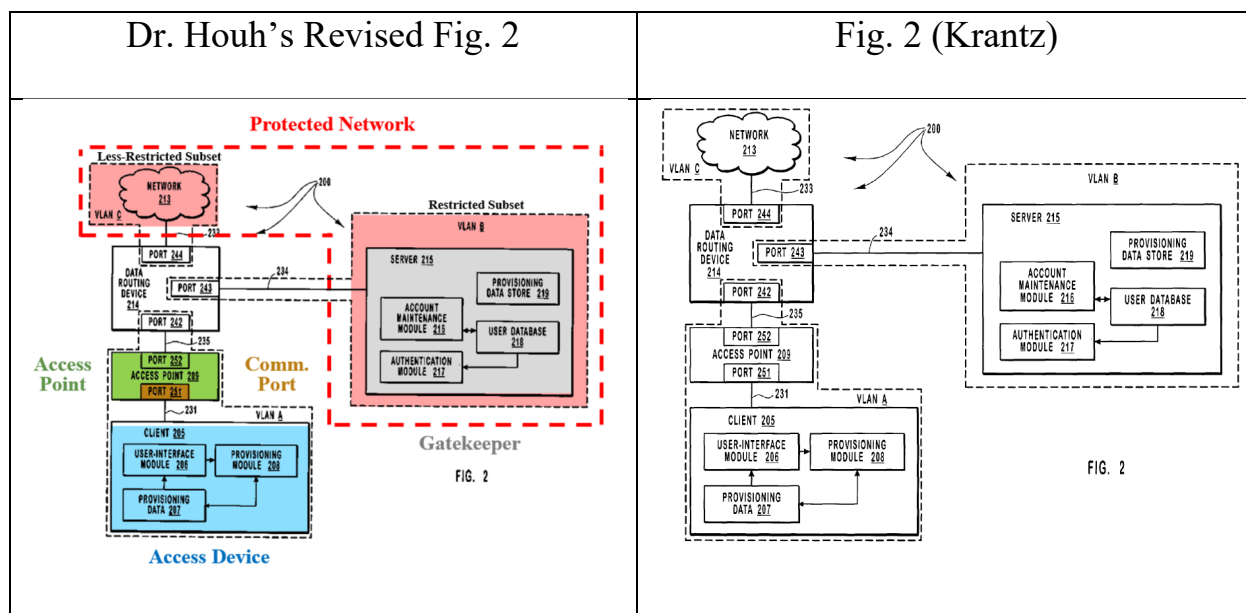
To try and show "subsets", Petitioner cobbles together Krantz's teaching of multiple *separate and distinct* networks. Petitioner's repackaging is nothing more than Krantz's Fig. 4 redrawn using the claimed invention as a blueprint.

³ This understanding is consistent with how POSITA understand EAP-Response/Identity. See EX2528.



Krantz has two separate and different networks—"Network 413" and "412". These are not subsets for the simple reason that they are not part of something else. Rather each network in Krantz is a separate network. Indeed, Petitioner admits this. Pet. at 22 ("the combination of second network VLAN C and first network VLAN B constituted a protected network."). Krantz confirms these two distinct networks: "a network architecture 400 that can provide access to a *first network* while restricting access to a *second network*." EX1205, [0030]; EX1205, [0060] ("data routing device 214 has been configured to separate network architecture 200 into VLANs A, B, and C.").

Regarding Fig. 2, Petitioner similarly misrepresents Krantz's actual disclosure by using the Patent as a blueprint for redrawing Fig. 2 to portray a "protected network" despite Krantz not reciting any "protected network."



As with Fig. 4, Krantz's disclosure of Fig. 2 recites separately "Network 213" and "Server 215." Petitioner is unable to point to any teaching in Krantz of subsets of a protected network. Indeed, Petitioner fails to point to any instance in Krantz where any of a "protected network" or network "subsets" is recited.

One must view a reference for what it teaches, not what it could have with hindsight knowledge—as Petitioner does—of the claimed invention. *Ortho-McNeil Pharmaceutical v. Mylan Labs.*, 520 F.3d 1358, 1364 (Fed. Cir. 2008). Petitioner's redrawn figures are of no moment.

With Krantz's Fig. 2, server 215 is disclosed as authenticating a user. EX1205, [0016]. Again, server 215 is not a "subset" of network 213. Instead, Krantz expressly states data routing device 214 is configured to separate network architecture 200 into VLANs A, B, and C, *i.e.*, three distinct networks. EX2565, ¶¶86-87; EX1205,

[0060]. Thus, server 215 fails to meet the “less-restricted subset of a network,” because Krantz has no subsets at all.

Recognizing Krantz's multiple networks communicating with one another are distinctly different from a network with subsets, Petitioner argues as a fallback that if the claimed "network" must be a single network, Krantz discloses this as well. Pet. at 38-50. Even if Krantz discloses a single-network embodiment, which is not explained in any detail with either Fig. 2 or Fig. 4, there is no disclosure of a less-restricted subset thereof. EX2565, ¶88. Further, Krantz's disclosure of authorizing a user to access a "selected computer system" says nothing about whether the network has restricted or less restricted subsets. *Id.*

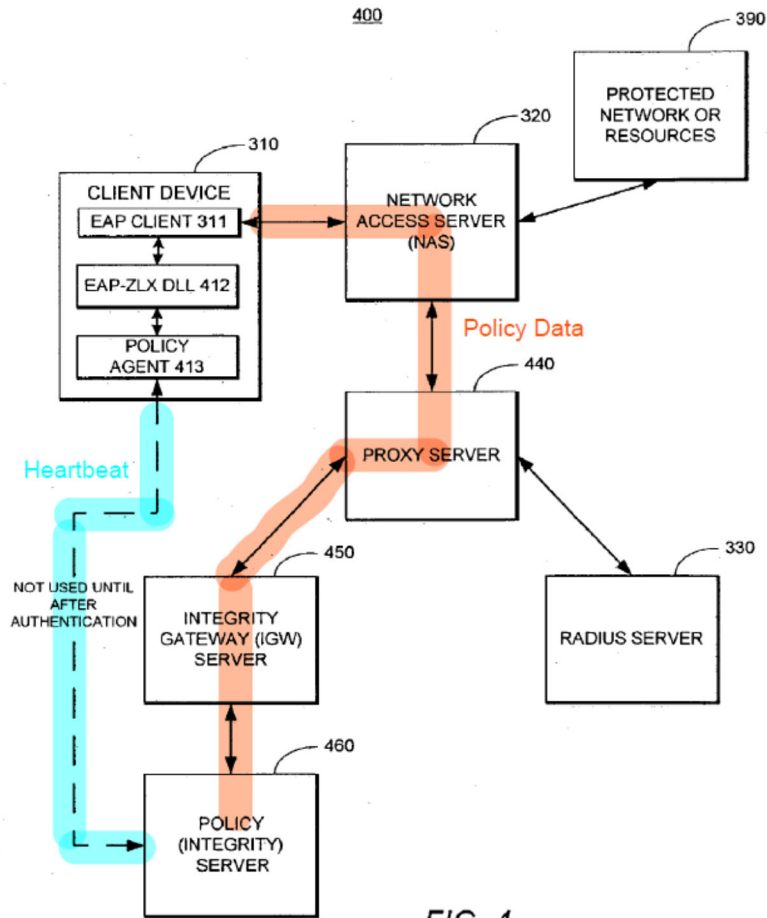
D. Krantz Does Not Disclose “Re-Auditing” or “Updated Audit Data”

Another reason why claim 22 is valid is because neither Krantz does not teach or suggest: [22.8] "***re-auditing*** the device in accordance to the security policy using the received ***updated audit data***." Pet. at 87-88. Here, the Petition relies exclusively on Krantz's "re-authenticate" disclosure. *Id.* ("[i]t may be that server 215 sets a session timeout, such as, for example, one hour, after which access point 209 will request client 205 to ***re-authenticate***." *Id.*, ("client 205 can ***re-authenticate*** in the background by submitting appropriate credentials to server 215.")). As discussed, not only does Krantz not teach "auditing" and "audit data," but it fails to disclose "re-auditing" and "updated" audit data.

The Petition does not rely on Herrmann for "re-auditing" and "updated audit data." Pet. at 87-88. This makes sense since Herrmann does neither. Petitioner might ask the Board to after-the-fact re-draft its Petition to include Herrmann's "IA_HEARTBEAT" disclosure. EX1206, [0080]. This would be improper. *See D3D Techs., Inc. v. Microsoft Corp.*, No. 2023-1462, 2024 WL 1433257, at *5 (Fed. Cir. Apr. 3, 2024).

Additionally, it would not work. Herrmann has a specific architecture for its policy approval process. This includes a proxy server, IGW server, and policy server that requires the policy data to be transmitted, "transform[ed]", and "reformat[ed]". EX1206, FIG. 7B-7C, 711-715. And once this process is complete, there is no indication of any additional audits. In fact, Petitioner cites to nothing in Herrmann suggesting the need for any further auditing after authorizing a device. EX2565, ¶164 ("A system would not continue to monitor (i.e. surveil) a trusted user or device, because that would be a waste of resources.").

Herrmann's heartbeat "status message" is separate from the policy-approval process. *See* EX1206, FIGS. 7B-7C and [0080]. For one thing, the "heartbeat" is "sent from the client directly to the policy server." EX1206, [0080]; *see also* Herrmann FIG. 4 (annotated below).



This is not re-auditing.

It also is not “updated audit data.” Rather, Herrmann’s “heartbeat” is just a “status message.” EX1206, [0080]. A status message does not contain substantive policy data but only carries minimal information to confirm an endpoint is connected. EX2565, ¶157. And this information is not used for evaluation or determining compliance with a security policy. *Id.*, ¶¶157-59. Indeed, as the term “heartbeat” suggests, it is known in the art to be merely an indicator that the client device is still active and has not left the network. *See, e.g.*, EX2569.

Herrmann's actual "policy data 616" is something else (EX1206, [0082], FIG. 6A), and is "collect[ed]," "receiv[ed]," "transform[ed]," and "reformat[ted]" in a very different way. *Id.*, FIGS. 7B-7C. Accordingly, neither reference discloses the claimed "re-auditing" or "updated audit data."

E. Dependent Claims 5-7

Claims 5-7 are also valid because neither Krantz nor Herrmann disclose a gatekeeper receiving "updated" audit data "after" configuring the access point.

- 5. The method of claim 2, further comprising ***receiving*** from the agent, ***updated audit data*** pertaining to the device ***after*** configuring the access point.
- 6. The method of claim 2, further comprising ***receiving***, from the agent, ***updated audit data*** pertaining to the device ***while*** the device has access to the less-restricted subset of the network.
- 7. The method of claim 2, further comprising ***continuing to receive at the gatekeeper***, from the agent, audit data pertaining to the device ***after*** the configuring of the access point.

As discussed above, neither Krantz's "re-authenticate" nor Herrmann's "heartbeat" constitutes "updated audit data." Accordingly, these claims are valid.

Additionally, however, neither Krantz nor Herrmann disclose "receiving"/"continuing to receive" this updated audit data "after" configuring or "while" access is granted.

The Petition merely concludes that "nothing in Krantz or Herrmann suggests the continued collection of audit data would cease..." Pet. at 80. Such speculative expansions of what Krantz or Herrmann ***could have*** disclosed, as contrasted by what

they *actually* disclosed is unavailing because one must view a reference for what it teaches, not what it could have with hindsight. *Ortho-McNeil*, 520 F.3d at 1364 (merely retracing the path of the inventor with hindsight and discounting the number of complexity of alternatives is insufficient to prove obviousness).⁴

F. Dependent Claim 12

Dependent claim 12 is also valid because Krantz does not disclose “audit data” that "concerns operating system of the device." The Petition relies solely on Krantz’s *authentication* disclosure of "a configuration sub-file to indicate a type of *EAP* used to *authenticate* a server with a client and/or to *authenticate* a client with a server... [an] element can be included in configuration sub-file to indicate whether or not operating system credentials should be used for *authentication*." Pet. at 84. As discussed, Krantz does not teach "audit data." Accordingly, claim 12 is valid.

The Petition does not rely on Herrmann, and therefore it should not be applied. *D3D Techs.*, 2024 WL 1433257, at *5.

But even Herrmann does not disclose this. Herrmann only teaches policy data for an "antivirus" software. This is different from, and does not concern the operating system of the device. EX2565, ¶167. Tellingly, the Patent treats these

⁴ As discussed in section VIII(B)(1), Petitioner itself discovered that its problems with network access control issues were too complex to solve on its own.

two things differently. EX1201, 11:53-56. And policy for an operating system has different evaluations than antivirus such as the “specific security patches installed.” EX1201, 6:52-53. In any event, the Petition provides no information on Herrmann or how its antivirus disclosure would in any way relate to the “operating system of the device.”

G. Dependent Claim 17

Claim 17 is also valid because neither reference teaches updating or remediation, *i.e.*, "the gatekeeper is configured to take part in bringing a software on the device up to date in response to applying the security policy."

The Petition relies on Krantz's "provisioning files [] for gaining full access to network 413." This fails for several reasons. First, "software incompatibilities" and "provisioning files" have nothing to do with—and thus are not "in response to"—"applying the security policy." Krantz's provisioning files are merely to configure devices with the necessary parameters and settings to connect to and operate on a network. For example, Krantz explains "[d]uring the registration process with the ISP, the computer system may download provisioning files for the wireless hotspot. Thus, upon connecting to the wireless hotspot, the computer system may already be appropriately configured for access the Internet through the wireless hotspot." EX1205, [0112]. Rather than the claimed “security policy,” these files ensure that

the device can access network services without requiring manual configuration by the end-user. EX2565, ¶¶170-71.

Second, even if "provisioning" files were "in response to applying the security policy," the claim requires the "gatekeeper is configured to take part in bringing a software on the device up to date." Petitioner's proposed gatekeeper of Krantz (e.g. RADIUS server 215) takes no part in administering provisioning files and the Petition does not say it does.

The Petition also relies on Herrmann's disclosure of: "a network administrator may require all users accessing the network to implement a virus definition update (e.g. DAT file)." Pet. at 85. But Herrmann also does not use the "gatekeeper" to perform any software update. Instead Herrmann explains that a person needs to do it: "The rules enforced by the policy server 460 may also be changed from time to time by a *user or administrator... a network administrator* may require all users accessing the network to implement a virus definition update (e.g., DAT file) that is targeted at a particular virus." Accordingly, claim 17 is valid for this additional reason.

VII. KRANTZ AS MODIFIED BY HERRMANN FAILS TO RENDER THE CHALLENGED CLAIMS OBVIOUS

A. All Claims

Each of the Challenged Claims require several limitations not taught by Krantz's authentication including: "applying a security policy that includes at least

one requirements pertaining to the audit data and at least one requirement pertaining to the authentication”, “sending a request for audit data”, and “receiving the audit data at a gatekeeper... the audit data pertaining to the device.” EX1201, claims 1 and 22. The evidence definitively shows why a POSITA would not want to, and in some instances, would not be able to, combine Krantz and Herrmann.

1. Petitioners Have Failed To Demonstrate The Combination

With respect to the combination, the Petition offers only bald rationales:

- “A POSITA would recognize that checking for anti-virus software would merely be an *additional item* for authentication module 217 (of server 215) to *check* in the authentication process already disclosed by Krantz.” Pet. at 59; Ex. 1203, ¶ 52.
- “Krantz’s authentication module, which *compares the credentials of a user against a database* (e.g., a user-identifier and password), as modified by Herrmann, would additionally *compare* a virus protection program on an access device against approved antivirus programs. Ex. 1203, ¶ 52.
- “... implementing these techniques into a combined Krantz/Herrmann system as doing would involve *minimal changes* to the existing Krantz system.” Pet. at 65.

Petitioner’s argument essentially distills to: Krantz says user authentication is good and Herrmann says device auditing is good, so one would be motivated to put them together by “checking” and “simple” or “minimal” software modifications. But Petitioners’ bald conclusion are divorced from the realities of the art.

First, Krantz and Herrmann are directed to different things. While Herrmann relates to network security, Krantz is directed to “automation” and “provisioning”;

not network security. EX1205, title, [0002]. Krantz is about reconciling “software incompatibilities” between a user device and network. E.g., Krantz seeks to enable a user device to automatically download ISP software. EX1205, [0020].

With regard to authenticating a user, Krantz merely references established authentication paradigms of user names, passwords, RADIUS protocols, and basic VLAN tagging. Indeed, Krantz’s touchpoints on authentication are little more than checking whether the user has an paid-up account with the ISP.

“It may be that a presented user-interface includes only “YES” and “NO” controls for authorizing further credit card payments or other electronic payment options.” EX1205, [0103].

“A user may be presented with an interface to enter information for registration (e.g., name, room number, credit card number, etc.). If the registration information is appropriate, the user can be authorized to access the Internet using the service.” EX1205, [0010].

None of this relates to the claimed invention’s application of “applying a security policy.” E.g., EX1201, 16:2-19, 16:61-17:12. Accordingly, Petitioner has failed to meet its burden.

The evidence demonstrates that Krantz and Herrmann would not be combined because, as the Patent explains: "The method used to support auditing functionality over the existing 802.1x protocol implementations is complicated and not an obvious variation of the 802.1x protocol." EX1201, 14:11-13. As Dr. Cole explains, authentication and auditing and/or applying a security policy to the access device was complicated. EX2565, ¶109-10. In particular, he explains that the security

infrastructure for authentication was distinct from that for security policy (or auditing) enforcement. *Id.* For example, authentication generally required a RADIUS server, supplicant, and authentication protocols. *Id.*, ¶¶111-13. These were incompatible with processing, analyzing, and handling policy information. *Id.*, ¶113. In contrast, auditing functionality (*e.g.*, applying a security policy to the access device) required a separate infrastructure. *Id.*

This complexity is the reason Petitioner tried, but could not implement a NAC solution for "applying a security policy that includes at least one requirements pertaining to the audit data and at least one requirement pertaining to the authentication." *See* Section VIII(A). It is also one of the reasons why InfoExpress took almost a year to conceive, work diligently, and reduce it to practice. *See* Section IX(D). Further, Krantz and Herrmann themselves confirm such a combination would make little sense. Accordingly, Petitioner failed to meet its burden demonstrating unpatentability based on the combination of Krantz and Herrmann.

2. Herrmann Confirms "Applying A Security Policy To The Access Device" Would Not Have Been "Minimal," "Simple", or Merely An "Additional Check" For Krantz's Server

Petitioner argues combining Herrmann with Krantz to meet the missing "audit" limitations would merely require "simple" and "minimal" modifications to Krantz's sever 215. Pet. at 19, 36. They provide no analysis or no reasoning. The only "evidence" of this is the conclusory statement by Dr. Houh unsupported by

anything other than his say-so. This should be disregarded. *cxLoyalty, Inc. v. Maritz Holdings Inc.*, 986 F.3d 1367, 1378 (Fed. Cir. 2021) ("We do not accord weight to conclusory expert testimony.")

Rather, Krantz's RADIUS server 215 analysis is basic. It receives a username and password, checks a database, and outputs an acceptance or rejection. EX1205, [0076]. This was well-known, and it required few resources. EX2565, ¶¶46, 107, 111-13, 120-21.

Tellingly, Herrmann has its own authentication "RADIUS server 330," and does not use it for policy enforcement. EX1206, FIG. 4. Rather than simply change the RADIUS 330 as shown in FIG. 3, Herrmann designs its own unique policy evaluation infrastructure. EX1206, FIG. 4 ("Policy (Integrity) Server 444," "Integrity Gateway (IGW) Server 450, Proxy Server 440). Herrmann's new policy infrastructure also adds a "policy agent 413" and custom EAP-ZLX extension. EX1206, (comparing FIGS. 3 and 4). The reason for this new policy infrastructure—as Herrmann suggests—is that you cannot modify the RADIUS server to evaluate a security policy of the access device. *See* EX2522⁵ (RADIUS Specification RFC

⁵ Herrmann incorporates RFC 2865 entitled Remote Authentication Dial In User Service (RADIUS) by reference. EX1006, [0009].

2865 stating: "A forwarding server MAY need to modify attributes to enforce local policy. *Such policy is outside the scope of this document...*")

Recognizing that this was not possible, Herrmann creates a complex infrastructure of servers, components, and its own proprietary protocols to conduct a policy evaluation.⁶ Herrmann needs a system of interconnected servers including a "Proxy Server," "Integrity Gateway Server," and "Policy Server." EX1206, FIG. 4. All of these are specifically designed to work with one another to "unwrap," (*id.*, [0082]-[0083], FIG. 7A, 708) "wrap," (*id.*, [0090], FIG. 7A, 705) "transform" (*id.*, [0095], FIG. 7B, 714), "reformat" (*id.*, [0096], FIG. 7C, 718), and send and receive various data packet transmission and messaging.

Not only that, but Herrmann creates a new and unknown proprietary data packet—EAP-ZLX—to transmit "policy data" within its construct of servers. EX1206, [0058], [0062], [0064]; EX2565, ¶¶125-27 (Cole saying EAP-ZLX is not known); EX2449, 259:9-275:9 (Houh agreeing that "EAP-ZLX" is not known).

⁶ Notably, while Herrmann's complex infrastructure discloses a policy evaluation, this infrastructure runs afoul of other key claim requirements including "configuring" the access point and auditing "while the device has access to a less-restricted subset of the network," *i.e.*, Herrmann doesn't solve the "bottleneck" issue.

The policy data in EAP-ZLX would be rejected by Krantz's RADIUS server 215. *See* EX2522 ("NAS is not required to implement all of these service types, and ***MUST treat unknown or unsupported Service-Types as though an Access-Reject*** had been received instead."); *see also* EX1206, [0096] (client deemed not in compliance if "the client does not have the required software installed enabling the client to negotiate the EAP-ZLX protocol.").

Dr. Cole confirmed this understanding and explained that infrastructures of authentication and policy evaluation were different and complex. Dr. Cole explains why in a typical policy evaluation, there are many types, different ways to check file histories and registries. EX2565, ¶113; *see also* EX2449, 195:4-197:20 & 246:19-247:24 (Dr. Houh testifying that there are "thousands" of networking protocols and each must be specifically designed to work with other components in the network).

Even if Krantz's server 215 could work with Herrmann, applying a security policy regarding antivirus software would not "merely be an additional item for authentication module 217 (of server 215) to check in the authentication process..." Pet. at 59; Ex. 1003, [0052]. A "check" would be insufficient. Rather, "applying a security policy to the access device" requires an evaluation that the anti-virus software is actually running and cannot be bypassed. In fact, mere "checking" results in the industry-wide problem of spoofing or the presenting of deceptive policy information.

Cisco itself admitted that RADIUS servers that merely "check" are susceptible. See EX2445, 1 (Cisco: "RADIUS Protocol under RFC 2865 is susceptible to forgery attacks by an on-path attacker who can modify any valid Response (Access-Accept, Access-Reject, or Access-Challenge) to any other response..."). Further, Cisco's early NAC attempt failed in part because of this problem. EX2446 ("Cisco's NAC can be fooled into thinking non-compliant PCs actually meet the security posture NAC is designed to enforce"); EX2447.

Accordingly, a POSITA would not be motivated to combine Krantz with Herrmann.

3. Herrmann's Client-Side System Teaches Away From Combination with Krantz's Server-Side System

Krantz and Herrmann would also not be combined together to meet the missing "audit" limitations because they disclose two different types of processing arrangements. Krantz describes centralized server analysis. Herrmann describes client-side analysis. They would not work together.

For example, Krantz's server 215 (the alleged "gatekeeper") is nothing more than a centralized RADIUS server. EX1205, [0058]. It receives authentication data originating from various client sources. Upon receipt, *the server processes* the authentication data. EX2565, ¶¶133, 148.

In contrast, Herrmann is a client-side solution. EX1206, [0062]. *The client device processes* the information. Through incorporation by reference⁷, Herrmann explains that for enforcement of anti-virus policies: **"In accordance with the present invention, a central filter is not employed. Instead, the present invention provides a client-side filter** that is controlled by the centralized authority as long as the centralized authority has a way of enforcing non-compliance." EX2521, 12:45-53. Thus, a centralized solution (e.g. non-client side)—like that in Krantz—would not work. EX2565, ¶¶140-51.

Herrmann explains the shortcomings of a server-side solution:

"Both strategies are based on a centralized filter mechanism, with most of the filtering work being performed at the server (as opposed to the individual client PCs). Such an approach is problematic, however. Because of the centralized nature of firewalls and proxy servers, each approach extracts **significant performance penalties**. During operation of a typical system employing either approach, a single server might have to do the filtering work for hundreds or even thousands of PCs or workstations. **This represents a major bottleneck to overall system performance.**" EX2521, 2:38-47.

"As another problem, *centralized filter architectures are missing vital information* to correctly interpret the data packets because the underlying protocols were designed for effective data transfer and not for data monitoring and interception. *Id.*, 2:59-63.

"There are still other disadvantages to centralized filtering. The approach is difficult to configure and administer. The task of setting

⁷ Herrmann incorporates US5987611 (EX2521) for explaining the ***"policy definition and enforcement"*** for, *inter alia*, ***anti-virus policies.***) EX1006, [0070].

up different rights for different users, workstations, or workgroups, for instance, is particularly difficult." *Id.*, 3:4-8.

A reference teaches away "when a person of ordinary skill ... would be discouraged from following the path set out in the reference, or would be led in a direction divergent from the path that was taken by the applicant." *Ricoh Co., Ltd. v. Quanta Computer Inc.*, 550 F.3d 1325, 1332 (Fed. Cir. 2008). Here, Herrmann specifically teaches away from including a device auditing function on a server based application, such as Krantz's authentication server.

This is hardly surprising from a technical viewpoint. There are critical differences between the codebases for client-side and server-side enforcement solutions. In particular, client-side codebase tends to be lightweight with lower processing memory. EX2565, ¶149. Server-side code is more intensive and requires significant resources. *Id.*, ¶150. In addition to defeating Herrmann's goal of defeating the centralized "bottleneck," combining these codebases would make little sense and not be compatible. Thus, it would not be obvious to combine Herrmann's client-side approach into Krantz.

VIII. OBJECTIVE EVIDENCE DEMONSTRATES NON-OBVIOUSNESS

Objective indicia of nonobviousness include: (1) commercial success, (2) copying, (3) industry praise, (4) skepticism, (5) long-felt but unsolved need, and (6) failure of others. *Transocean Offshore Deepwater Drilling, Inc. v. Maersk Drilling U.S., Inc.*, 699 F.3d 1340, 1349-56 (Fed. Cir. 2012). "[E]vidence of

secondary considerations may often be the most probative and cogent evidence in the record. It may often establish that an invention appearing to have been obvious in light of the prior art was not." *Transocean*, 699 F.3d at 1349.

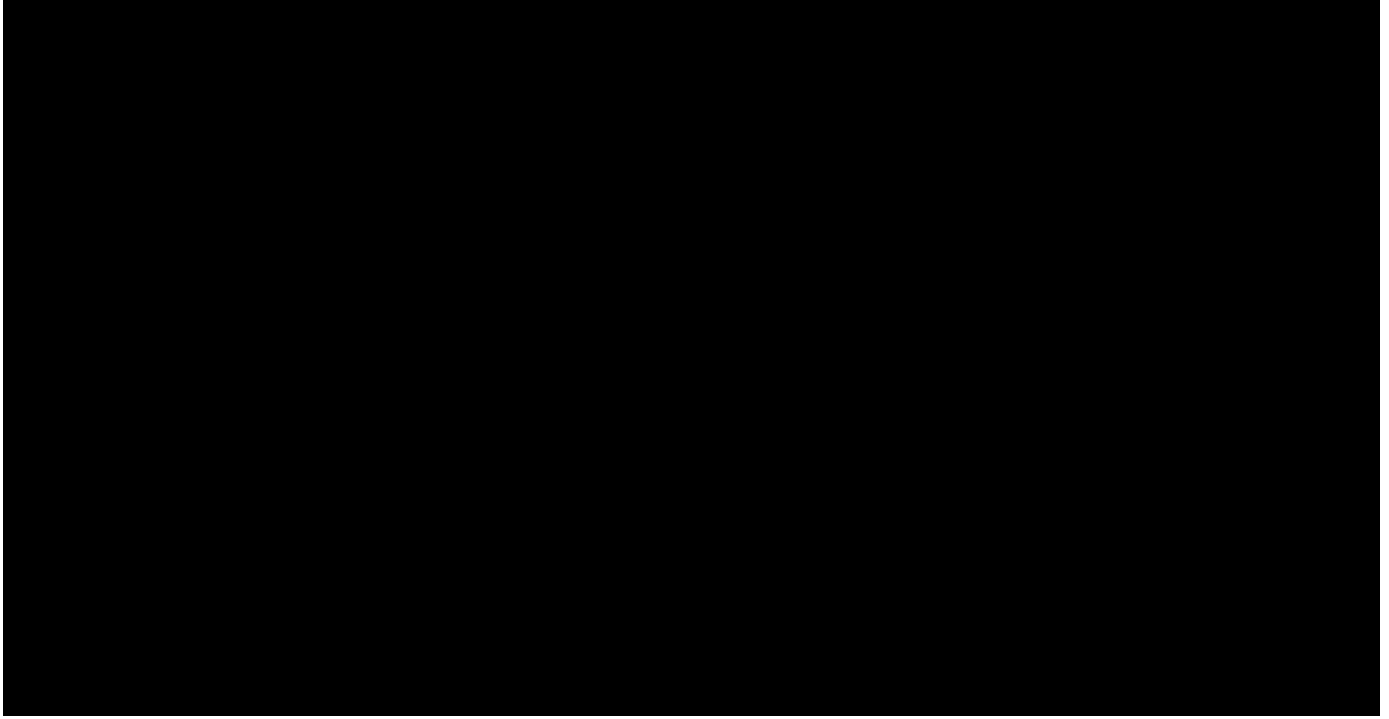
There must be nexus between the merits of the claimed invention and the objective evidence. *Volvo Penta of the Ams., LLC v. Brunswick Corp.*, 81 F.4th 1202, 1210 (Fed. Cir. 2023). Nexus is typically shown by: (1) a presumption, or (2) direct evidence of the unique characteristics of the claimed invention. *Id.* A patent owner is entitled to a presumption of nexus if the patentee shows the asserted evidence is tied to a specific product and the product "is the invention disclosed and claimed." *Fox Factory, Inc. v. SRAM, LLC*, 944 F.3d 1366, 1373 (Fed. Cir. 2019).

A. At the Time of the Invention and at Present, InfoExpress's Products Embody the Claimed Inventions and are Coextensive with the Patent.

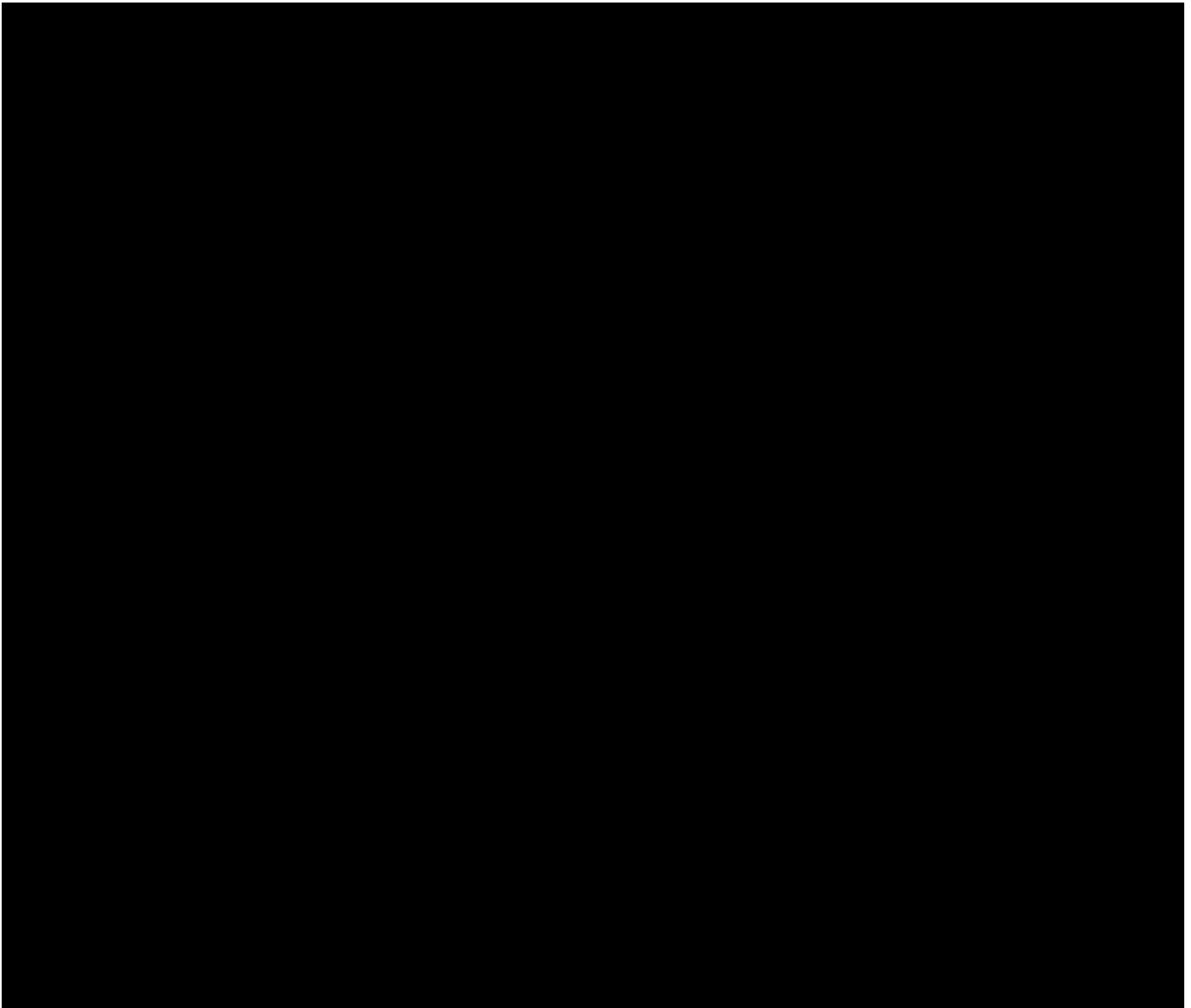
InfoExpress's CyberGatekeeper LAN ("CG LAN") and CGX products embody the claims of the '444 Patent and are coextensive with them. EX2427, ¶¶44-46 and Appx. C (claim chart). To be sure, the CG LAN and CGX products are marked with the InfoExpress patents. EX2451-EX2457; EX2459-2468. Accordingly, there is presumed nexus between the secondary consideration evidence below and the 'Patent claims.

In addition, the evidence demonstrates Petitioner's own failure, praise, and copying, is narrowly targeted to not only the claim limitations themselves, but to the

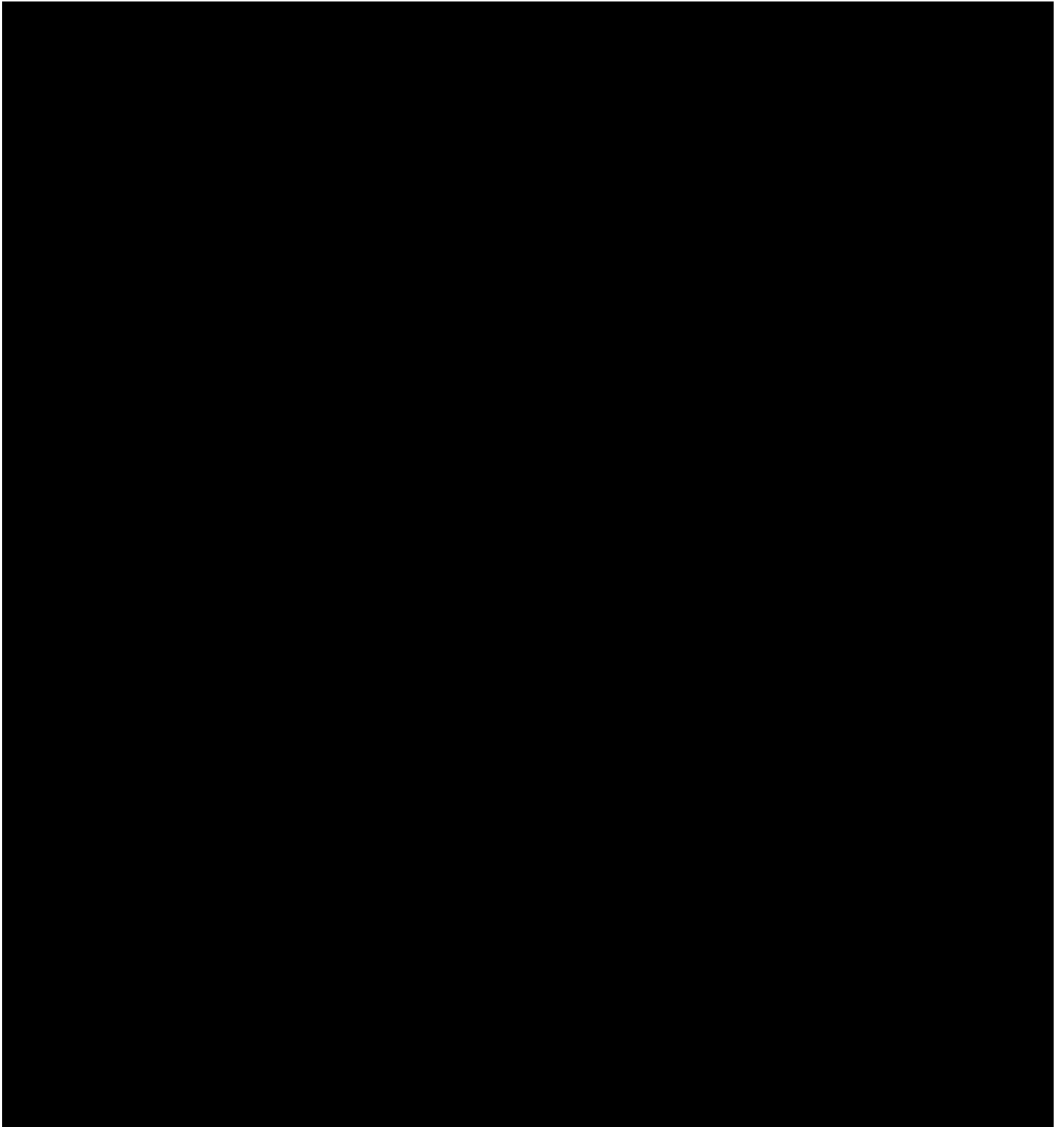
inventive combination of claim elements that Petitioners concede are missing in Krantz and supplied by Herrmann, including “applying a security policy that includes at least one requirements pertaining to the audit data” (claims 1, 22) (Pet. at 57), “updated audit data pertaining to the device” (claims 5, 6) (Pet. at 77-80), “continuing to receive . . . audit data pertaining to the device after the configuring of the access point” (claim 7) (Pet. at 80), “audit data pertaining to an application” (claim 10) (Pet. at 81), “audit data . . . concern[ing] [the] operating system of the device” (claim 12) (Pet. at 83), and “bringing [] software on the device up to date” (claim 17) (Pet. at 85).⁸



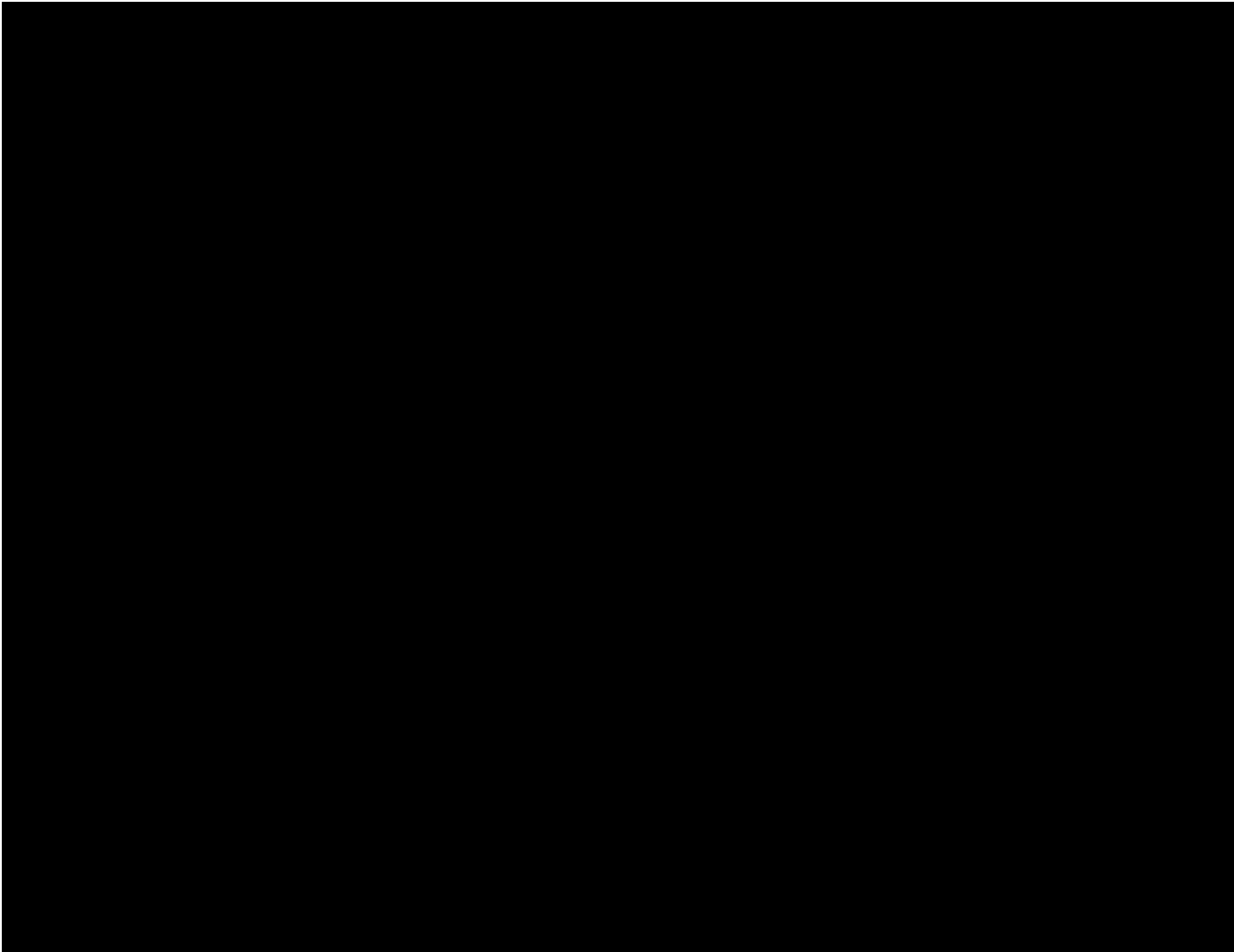
⁸ Additionally, and as explained, Krantz does not disclose or suggest “A method for auditing a device” or “audit data.”



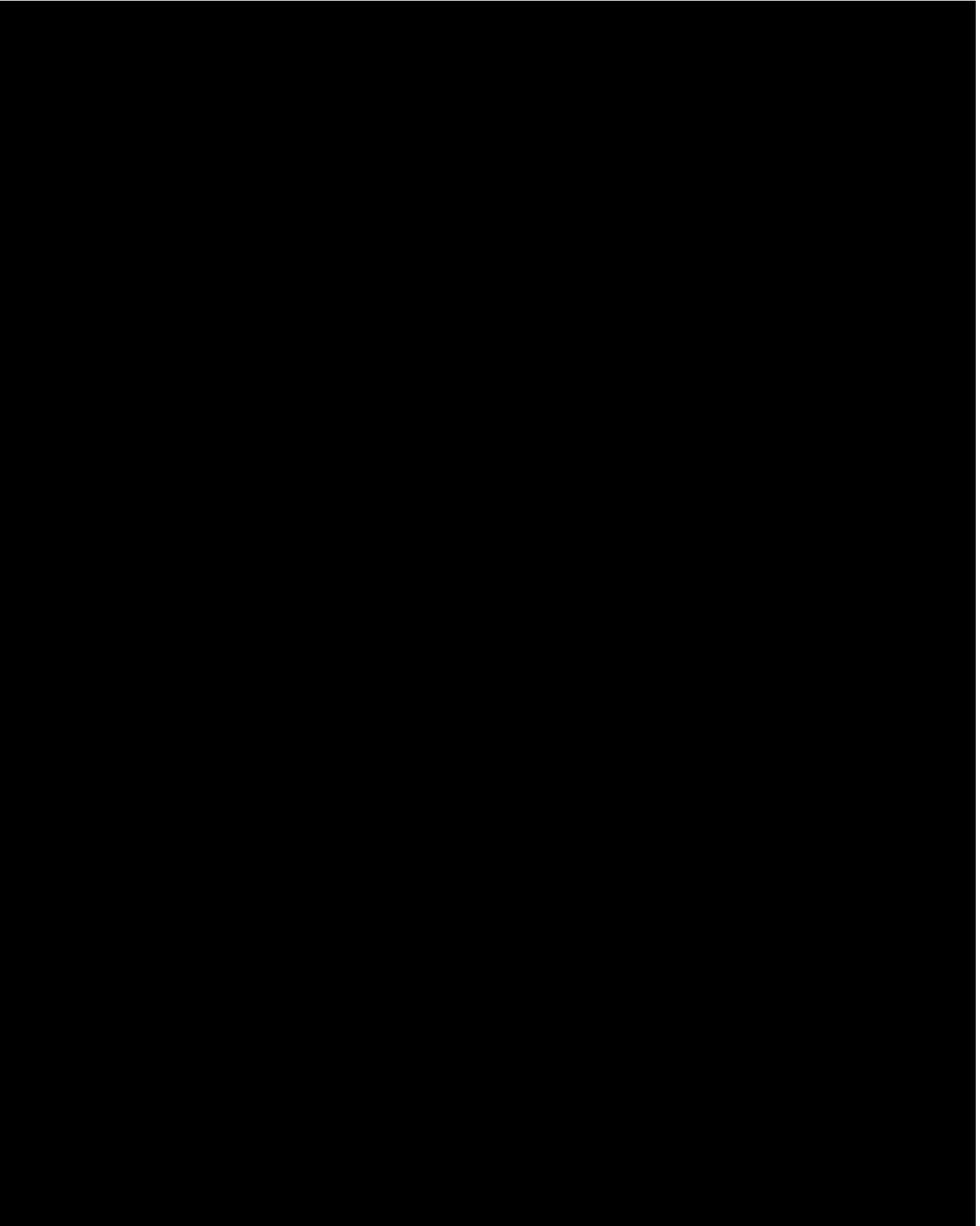
⁹ The claims of the Patent are directed to both authentication and auditing in accordance with a security policy. *E.g.*, claims 1, 22 (and dependents) (“applying a security policy that includes at least one requirements pertaining to the audit data and at least one requirement pertaining to the authentication”) claims 10, 12 (audit data).

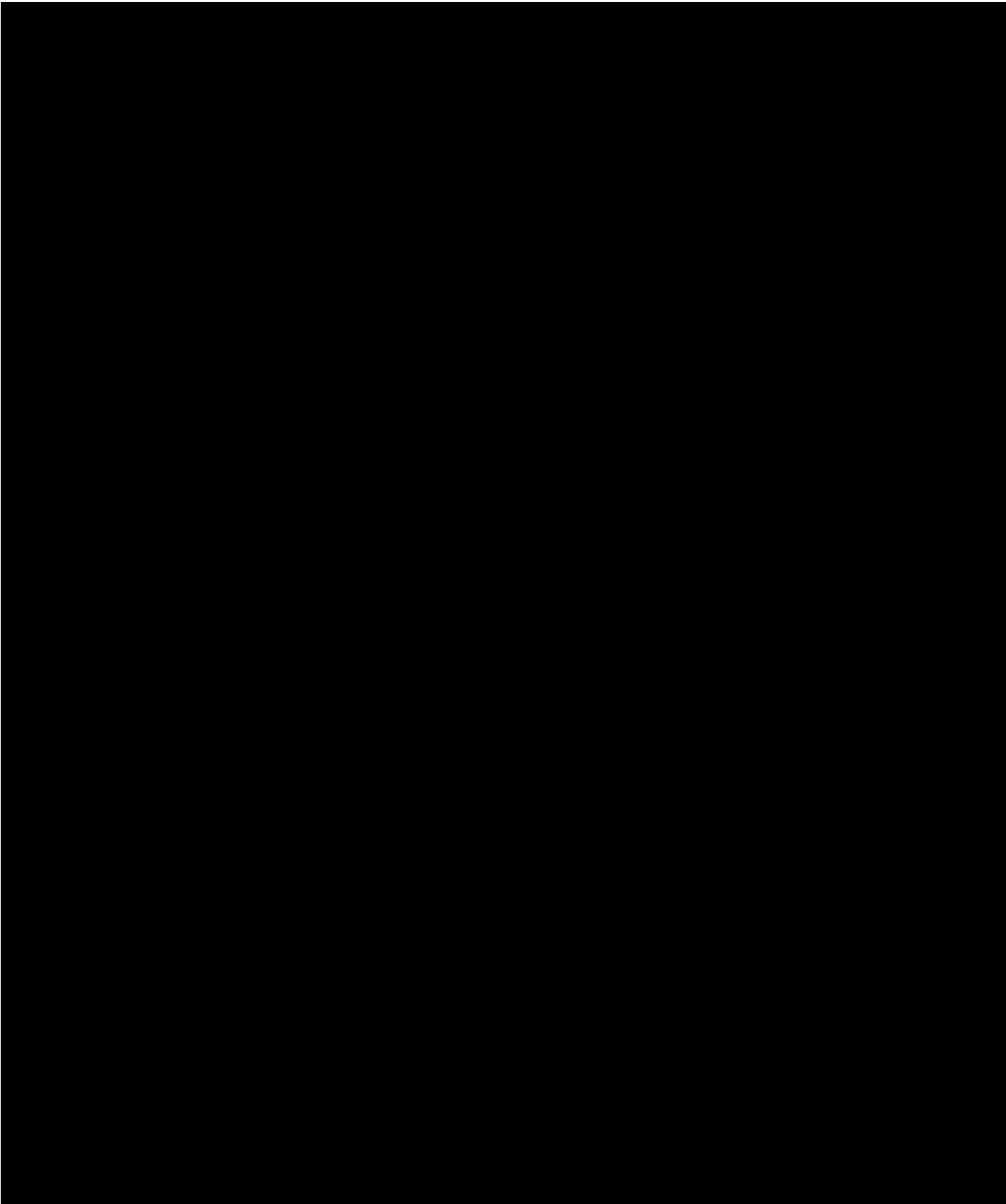


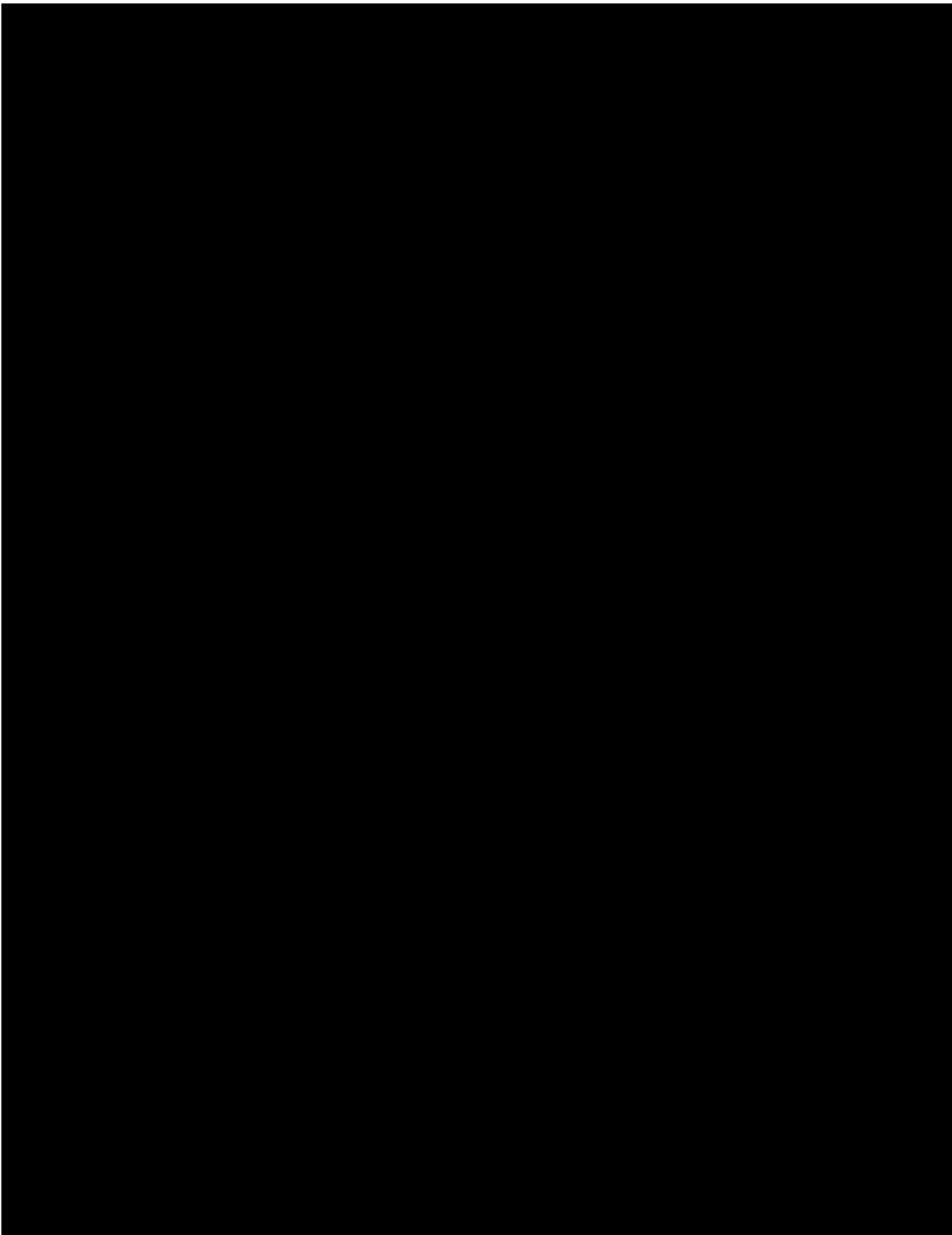
¹⁰ Such industry praise from Cisco itself (a top potential competitor) is further evidence of nonobviousness. *Apple Inc. v. Samsung Elecs. Co.*, 839 F.3d

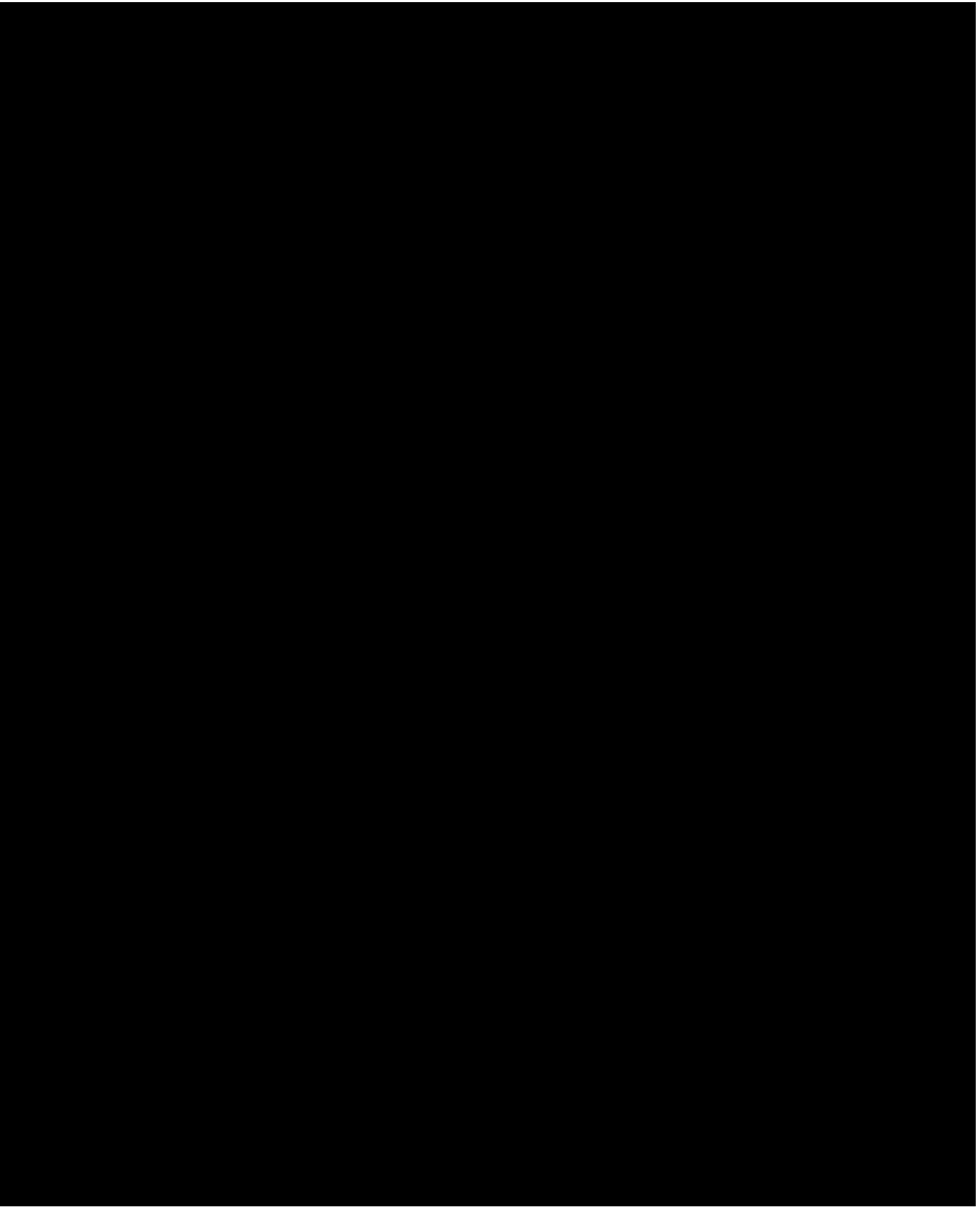


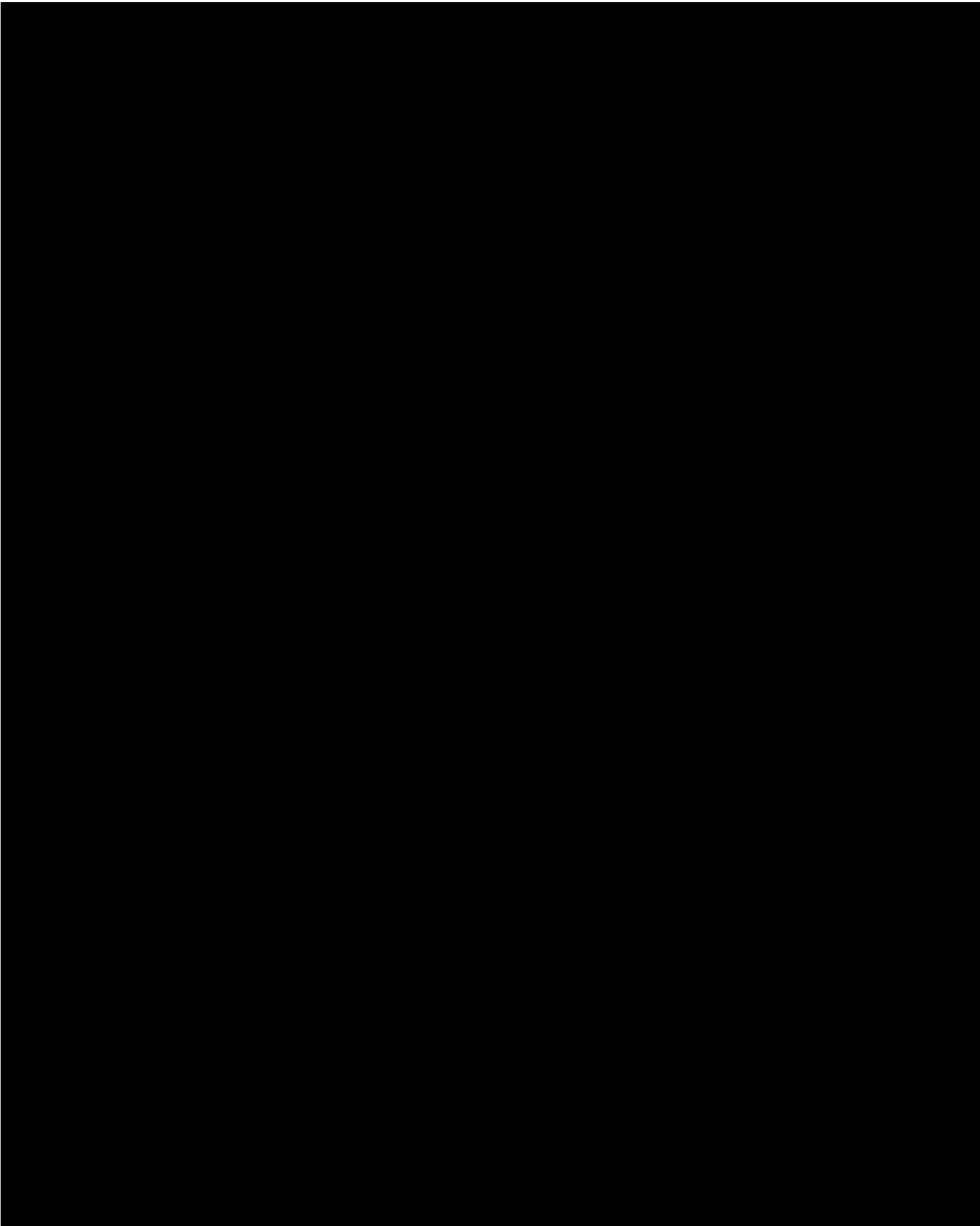
1034, 1053 (Fed. Cir. 2016) (“if there is evidence of industry praise of the claimed invention in the record, it weighs in favor of the non-obviousness of the claimed invention,” and further stating that “internal documents from the patentee’s top competitor represent important admissions, *acknowledging the merits of the patented advance over the then state of the art* and can be used to establish industry praise”); EX2470 (Cisco: “InfoExpress appear[ed] quite far along in [its] product development.”)

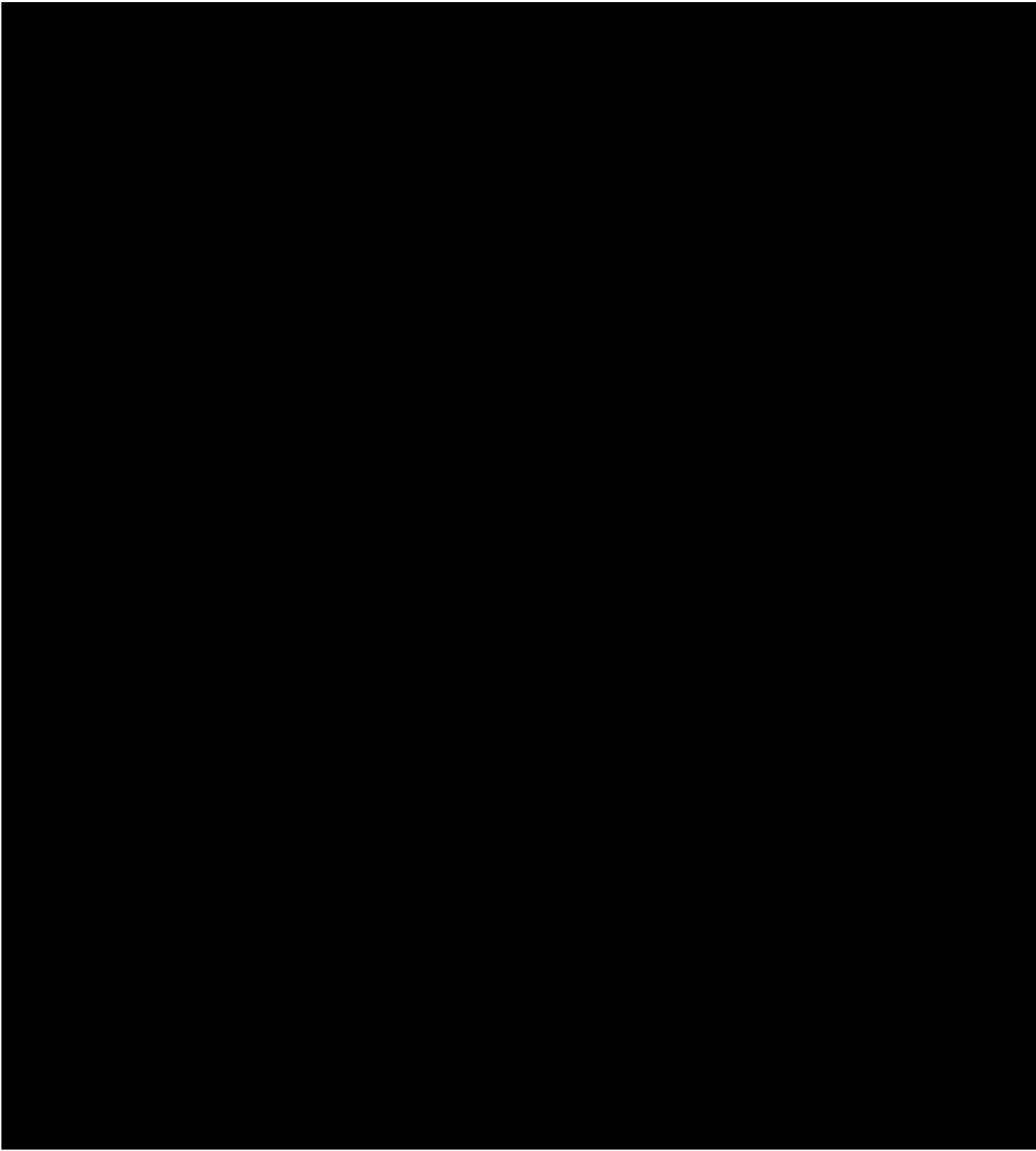




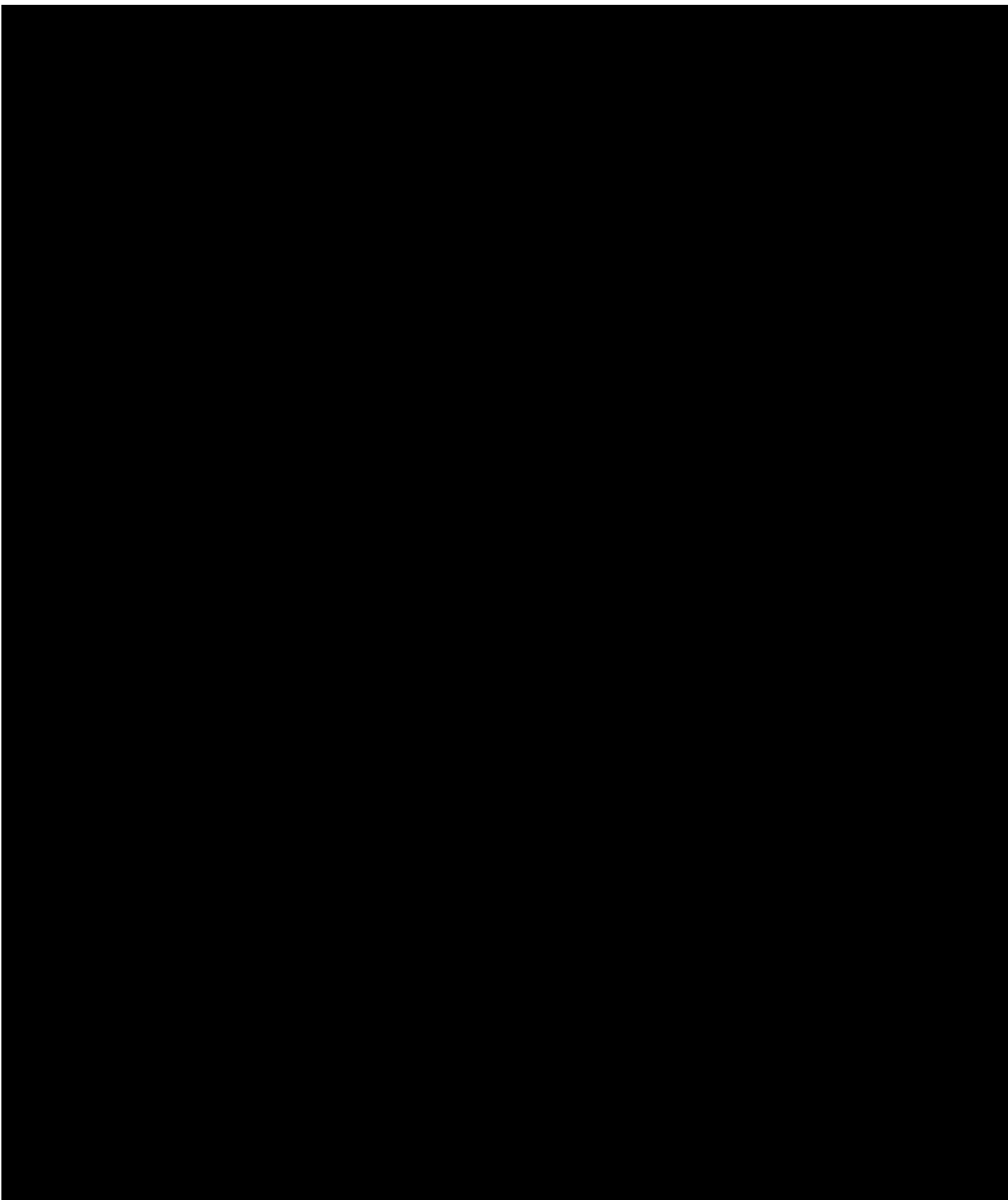


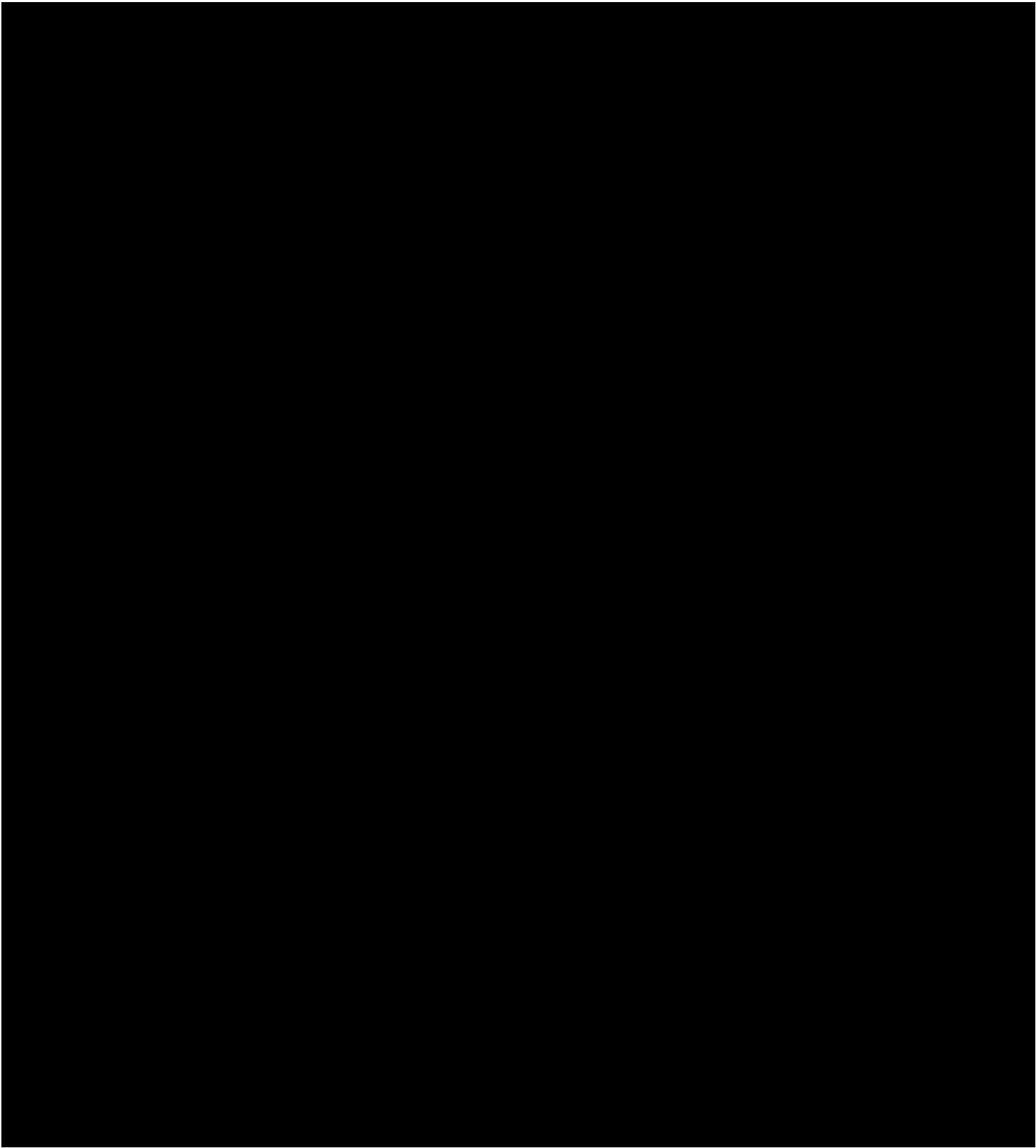


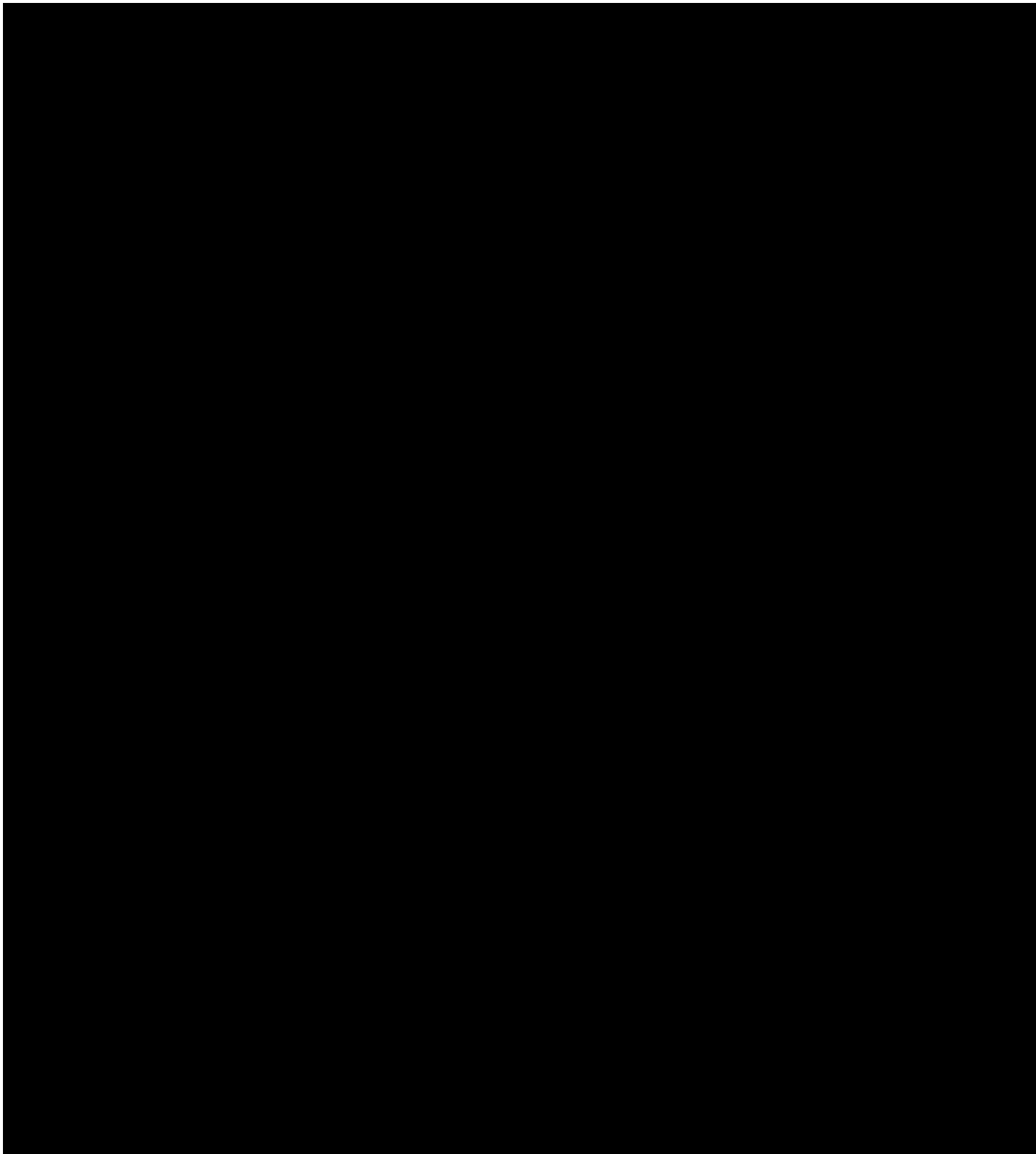




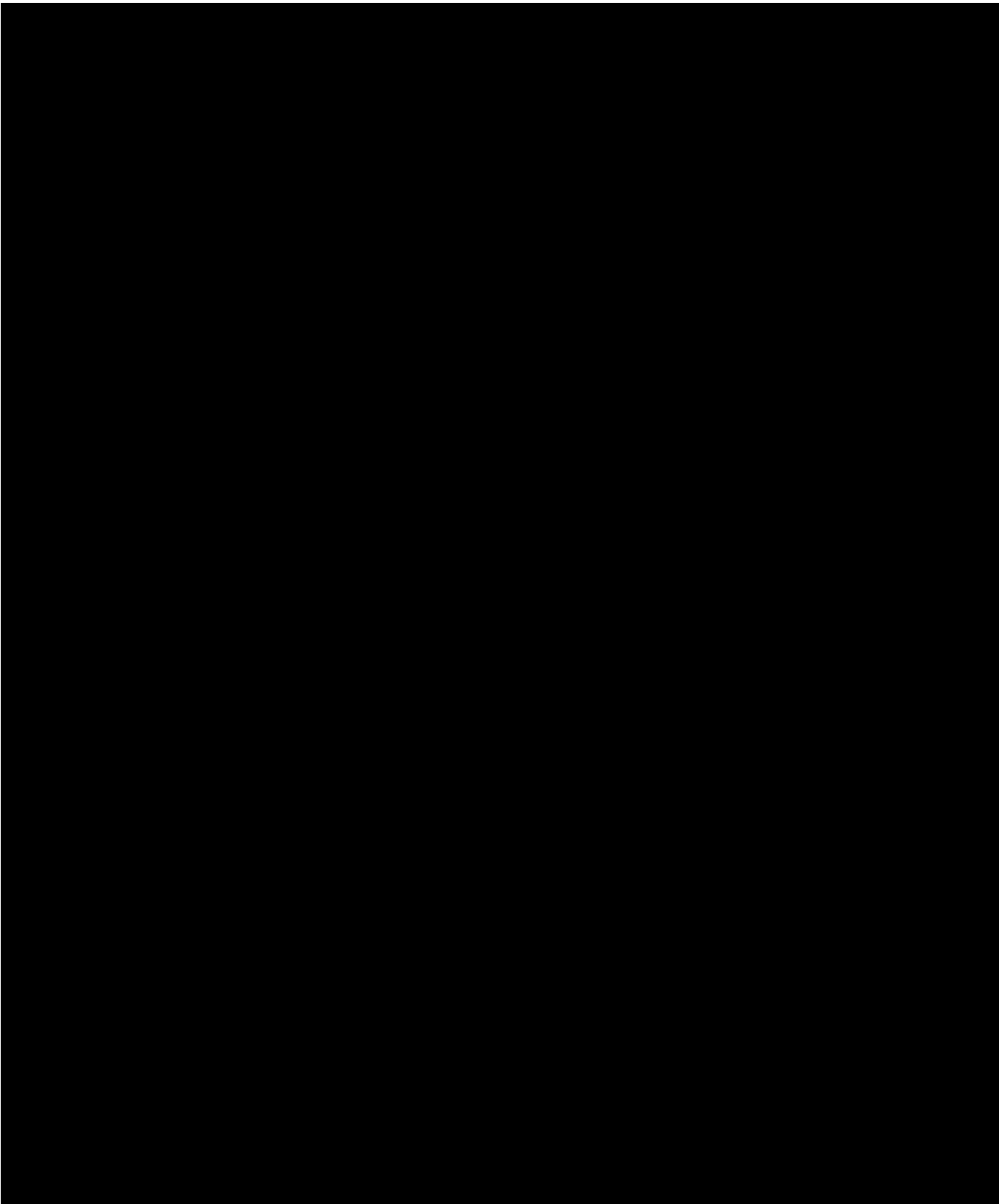
¹¹ *See also* EX2485; EX2486 at 14-17; EX2487; EX2488.





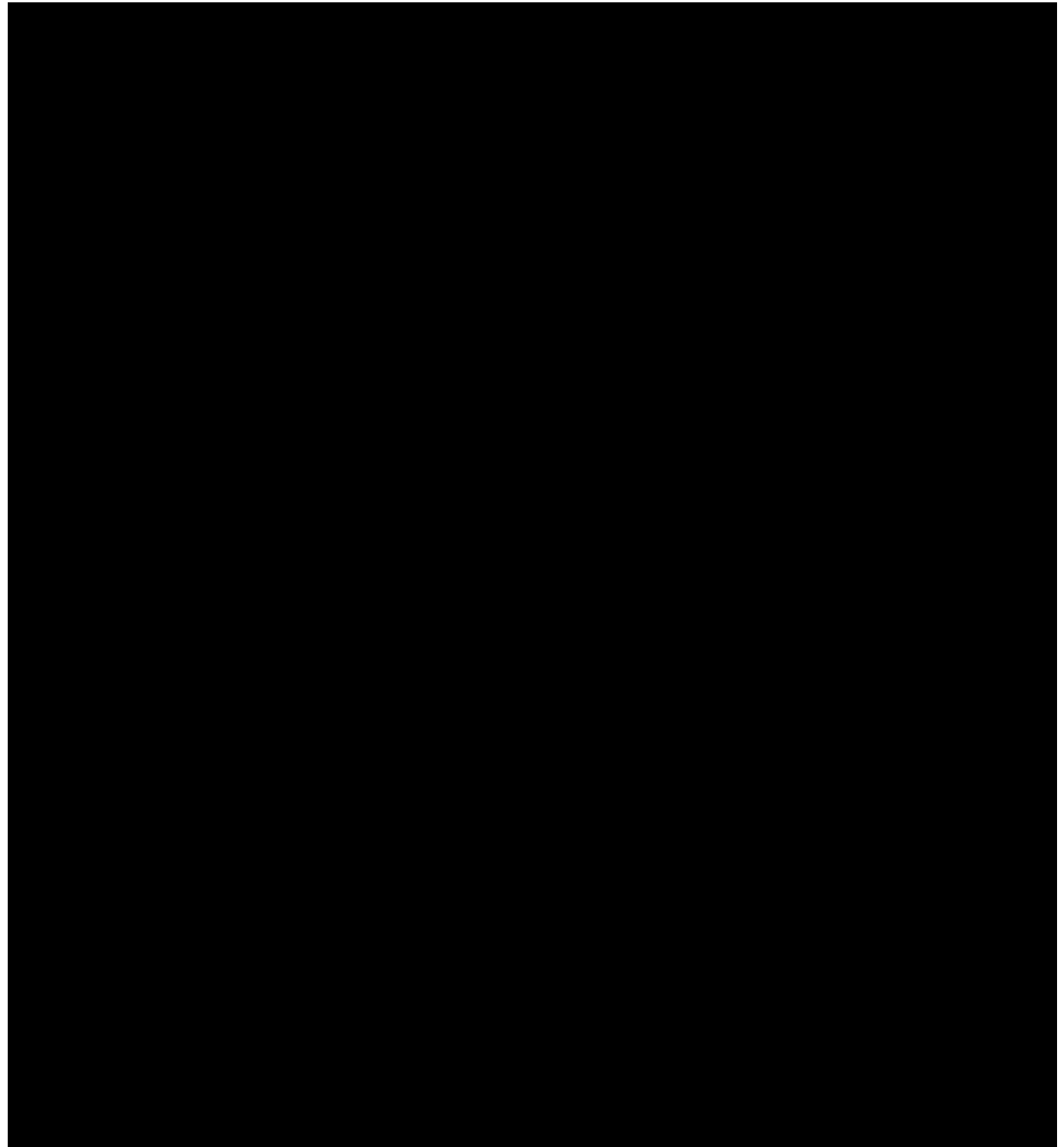


¹³ EX2420; EX2421; EX2493-EX2495 (documents relating to interoperability testing by KeyLabs).

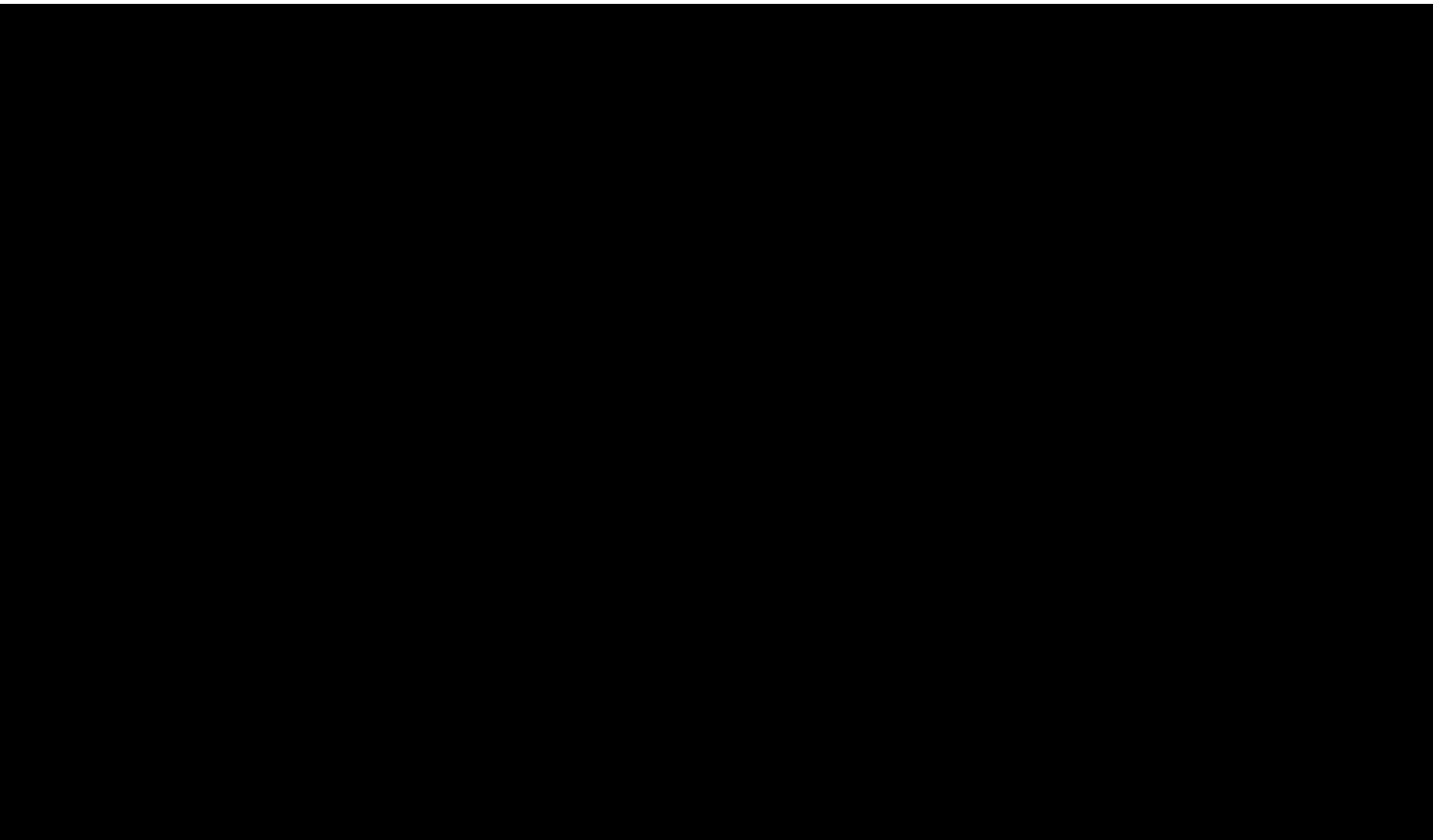


¹⁴ *Also* EX2501 (cover email).

¹⁵ *See also* EX2505 (Cisco acknowledgement); EX2506 (Cisco: “testing passed”); EX2507 (invitation to CDTP).

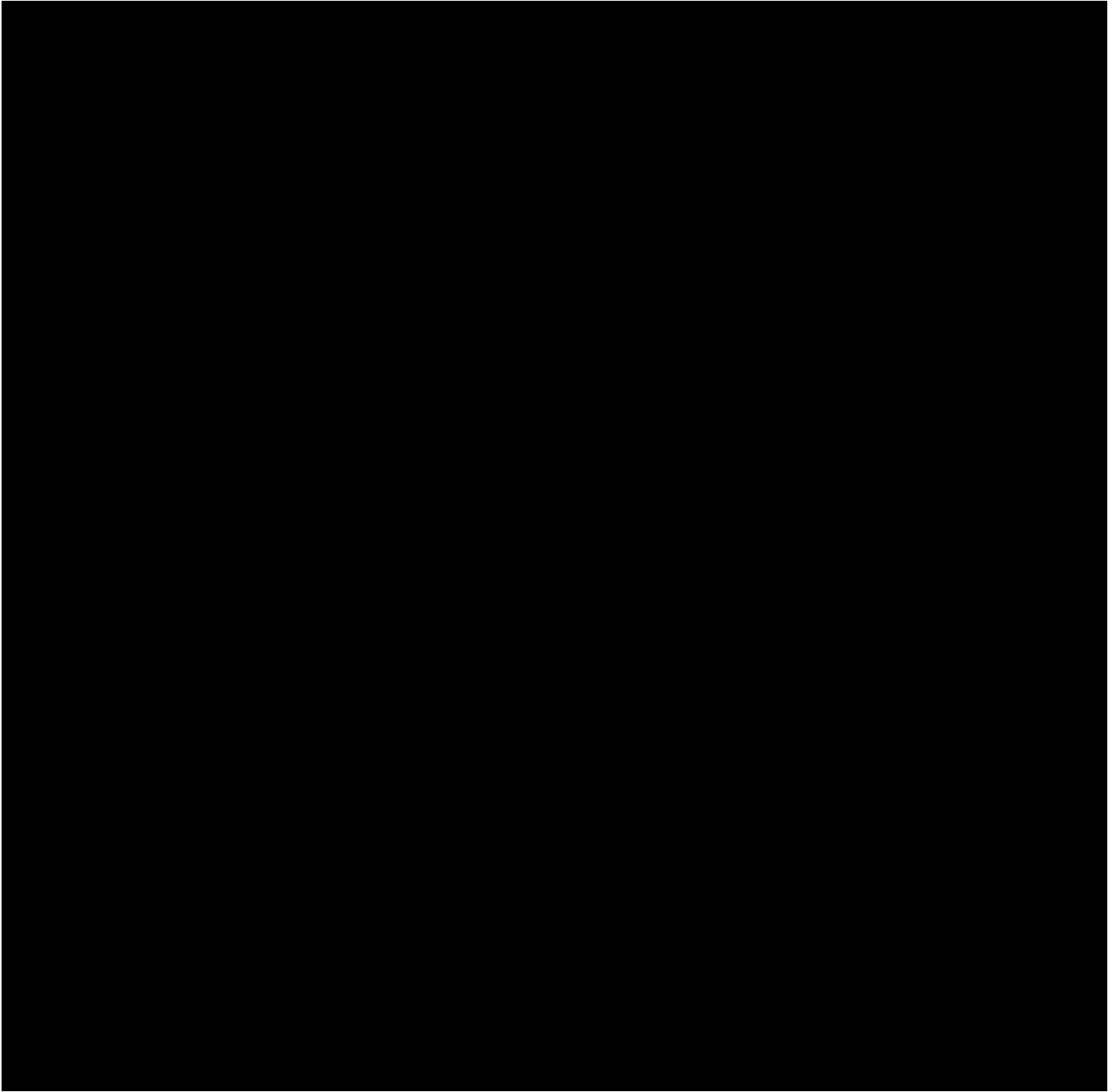


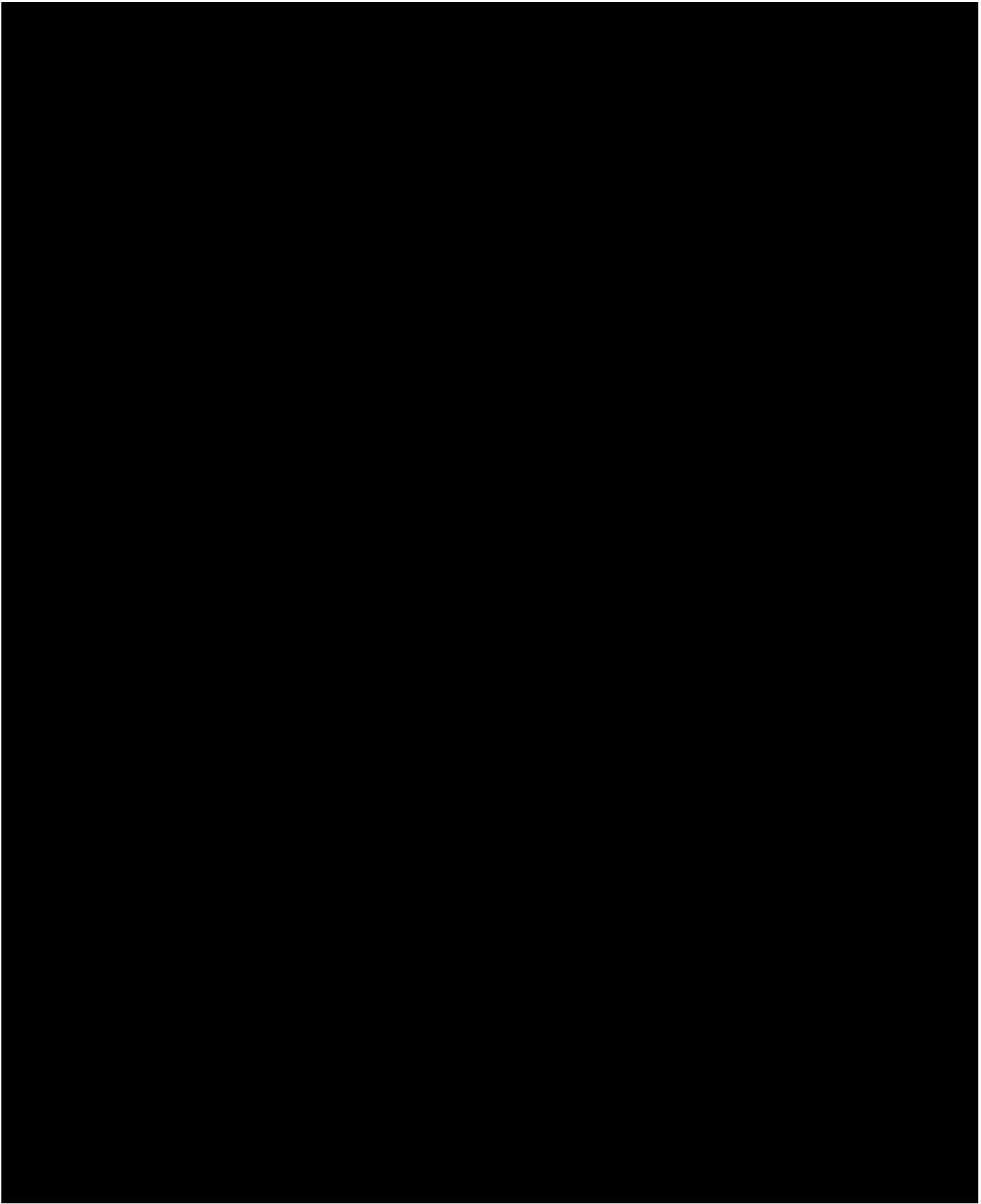
¹⁶ Citing EX2530, EX2551, EX2552, EX2531, EX2532-EX2540; EX2550; EX2553; EX2554.

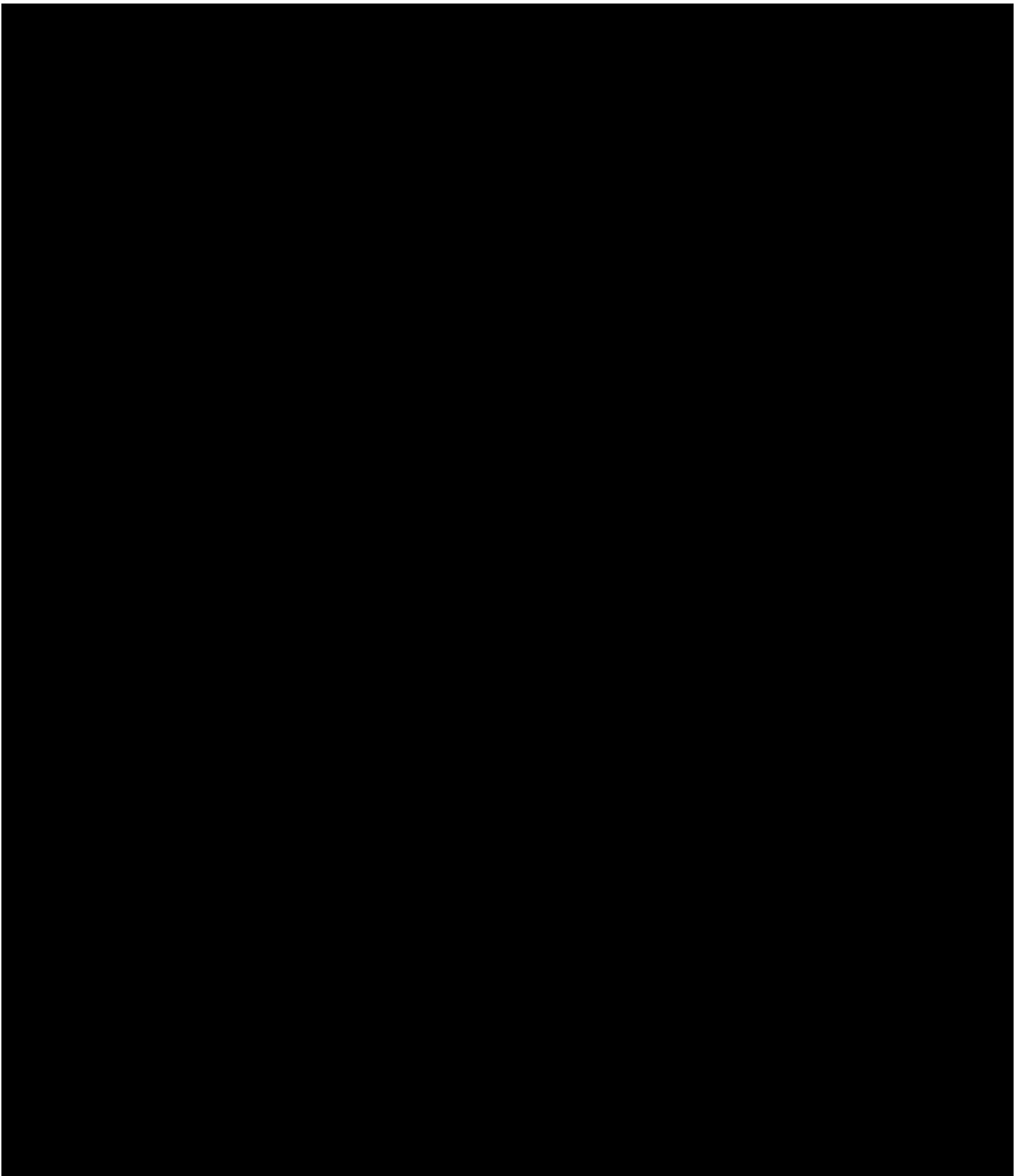


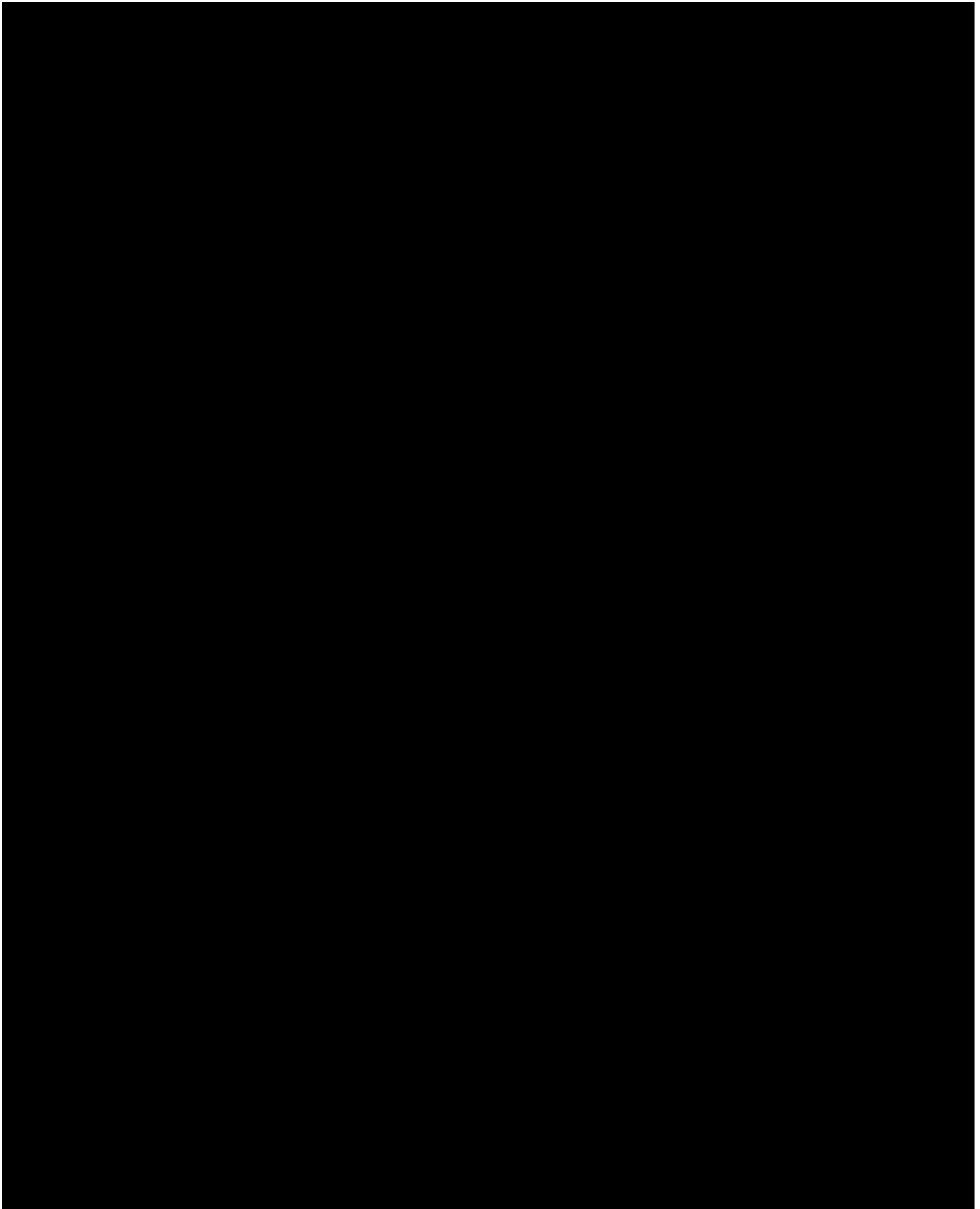
¹⁷ Cisco had multiple occasions to observe the CG LAN, including at least:

- **The NAC Developers Conference** in December 2004. EX2508; EX2509.
- **The Systems Engineer Virtual Team (SEVT)** in April 2005. EX2510; EX2511.
- **Networkers World of Solutions** in June 2006. EX2512-EX2514.
- **Cisco Networkers EMEA** in December 12-15, 2005. EX2515; EX2516.
- **Cisco Networkers Live 2007**. EX2517.









[REDACTED]

[REDACTED]

[REDACTED]

IX. ALL GROUNDS: NEITHER REFERENCE CONSTITUTES PRIOR ART

Neither reference constitutes prior art because the inventors conceived of the inventions before the effective dates and exercised reasonably continuous diligence in reducing the inventions to practice.

A. Legal Standard

A reference is prior art only if filed before the date of "the invention by the [patent owner]." 35 U.S.C. § 102(e) (pre-AIA).

To antedate a reference, one must show conception prior to the critical date and "reasonably continuous diligence" throughout the critical period from just before the effective date of the reference until reduction to practice (RTP). *ATI Techs. v. Iancu*, 920 F.3d 1362, 1369 (Fed. Cir. 2019). "No general standard, by which diligence can be estimated, has been established by the law, nor, in the nature of things, is such a standard possible." *Id.* at 1374.

For reasonably continuous diligence, an inventor need not work on reducing the invention to practice daily, and periods of inactivity do not automatically vanquish a claim of reasonable diligence. *Id.* at 1369. An attorney's work preparing

a patent application can demonstrate diligence. *Perfect Surgical Techniques v. Olympus America*, 841 F.3d 1004, 1009-1012 (Fed. Cir. 2016).

Inventor declarations submitted to establish conception and diligence must be corroborated. *Id.* at 1007. The "rule of reason" analysis governs whether corroboration is sufficient. *Id.* at 1009. "A variety of activities may corroborate an inventor's testimony of reasonable diligence, and such corroborating evidence is considered 'as a whole.'" *Id.* at 1007-08 (quotation omitted). The patent owner need not corroborate every contested factual issue, but instead merely needs to produce sufficient independent circumstantial evidence to support the testimony. *Id.* at 1009.

The purpose of diligence is to show that the invention was not abandoned, set aside, or unreasonably delayed, not to "scour the patent owner's corroborating evidence in search of intervals of time where the patent owner has failed to substantiate some sort of activity." *Id.*

B. The Inventors Conceived of the Inventions Before Critical Dates.

Petitioner asserts Krantz's effective date is December 6, 2002 (Pet. at 7) and Herrmann's effective date is March 13, 2003.¹⁸ *Id.* at 10. InfoExpress conceived of the claimed invention earlier.

¹⁸ Herrmann's provisional date is listed as December 2, 2002. Petitioners waived any right to establish an earlier §102(e) date because they failed to analyze its provisional

On November 14, 2002, co-inventor Lee e-mailed "CyberGatekeeper LAN Based Policy Enforcement Engineering Specification" (EX2011) demonstrating that the claimed inventions were conceived of by then. EX2012; EX2564 (Supplemental Lum Declaration), ¶12; EX2520; EX2429 (Lee Declaration), ¶13.

Conception is demonstrated in Dr. Smith's claim chart mapping EX2011 to the Challenged Claims as set forth in EX2009.

[REDACTED]

filing in the Petition. Notwithstanding, Herrmann's provisional date is still later than the November 14, 2002 conception and is not prior art regardless.

1. InfoExpress Exercised Reasonably Continuous Diligence Up and Through Constructive RTP.

InfoExpress exercised reasonably continuous diligence up to and through at least the filing of Provisional Application 60/513,080 on October 21, 2003. The filing of that application constitutes constructive RTP. Section IX(d); EX2007; EX2010.

On October 7, 2002, inventor Stacey Lum told the InfoExpress team:

"All, It may be possible to use 802.1x to audit [enforce] a system rather than switching them between VLANs. There's an authentication specific component in 802.1x, so we might be able to use that instead of VLANs." EX2015; EX2016.

This was groundbreaking because preexisting security technologies did not include implementation of auditing support functionality over authentication protocols such as 802.1x.

InfoExpress diligently reduced the inventions to practice from conception until constructive RTP on at least October 21, 2003. Diligence is shown by evidence including:

- i. emails;
- ii. technical specifications and analyses; and
- iii. the declarations of InfoExpress CEO Stacey Lum (EX2564) and Alice Lee (EX2429).

As further detailed in the diligence calendar (EX2004), InfoExpress worked consistently to reduce the claimed invention to practice. This evidence leaves no doubt that the InfoExpress inventors conceived of and diligently pursued RTP during the critical period. *See ATI*, 920 F.3d at 1373 (finding that Patent Owner's evidence did "not point to the remotest suggestion of abandonment or setting aside" where a calendar demonstrated activity on majority of days in diligence period and declaration summarized documents in support of diligence); *Monsanto*, 261 F.3d

at 1369 (substantial diligence evidence where the Patent Owner identified record evidence showing activity multiple times per month during the critical period, and there was no reason to doubt that activity was relevant in reducing invention to practice).

[REDACTED]

1 [REDACTED]

[REDACTED] [REDACTED]

[REDACTED]

1 [REDACTED]

[REDACTED]

[REDACTED]

1 [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

1 [REDACTED]

[REDACTED]

1 [REDACTED]

[REDACTED]

□ □ □ □ □

114

████████████████████

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
[REDACTED]
- [REDACTED]
[REDACTED]
- [REDACTED]
[REDACTED]
- [REDACTED]
[REDACTED]
- [REDACTED]
[REDACTED]
- [REDACTED]
[REDACTED]
[REDACTED]
- [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
- [REDACTED] [REDACTED]
[REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

I [REDACTED]
[REDACTED] [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

I [REDACTED]

[REDACTED]

I [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

I [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[illegible]

[illegible]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

■ [REDACTED]

[REDACTED]

■ [REDACTED]

[REDACTED]

■ [REDACTED]

[REDACTED]

■ [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

■ [REDACTED]

[REDACTED]

■ [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

■ [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

■ [REDACTED]

[REDACTED]

- [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
- [REDACTED]
[REDACTED]
- [REDACTED]
- [REDACTED]

2. The Inventors Achieved a Constructive RTP by Filing U.S. Provisional Patent Application Serial No. 60/513,080 on October 21, 2003.

As discussed by Dr. Smith (EX2007 & EX2010), the '080 Provisional provides support for the Challenged Claims in accordance with pre-A.I.A. 35 U.S.C. §§ 119(e) & 112, ¶ 1.

For example, EX2006 explains “The invention is directed to controlling access to a corporate network based on audit criteria for end points”. EX2010 at 1-3. “[P]ages 8 through 11 (and Figures 4, 5a, and 5b therein) all describe authentication being conducted, for example using the Extensible Authentication Protocol (EAP)”. EX2010 at 3-7. “[P]ages 3 and 9 (and Figure 4 therein) all

describe authentication being conducted, for example using [EAP] with a device connected ‘via a computer network to an access point configured to use an 802.1X protocol’”. EX2010 at 7-12. “[T]here is an ‘auditing protocol’ which ‘calls for audit information,’ i.e., ‘audit data’ from the ‘agent on the EP,’ i.e., the ‘agent running on the device’”. EX2010 at 13-15. “[T]he audit data is sent from the PC (device) through the Access Point (AP) to the GK (gatekeeper).” EX2010 at 16-19. “If the EP’s audit information complies with the policies, the GK lets the EP access the corporate network.” EX2010 at 20-28.

Regarding [22.8], “the appendix figure on page 21 explains [] that the ‘system is audited and re-audited’”. EX2010 at 61-63 (cleaned up).

As demonstrated above and in further detail in EX2010, the inventors achieved conception and RTP as of the filing of the provisional patent application.

X. CONCLUSION

For these reasons, Patent Owner respectfully requests the Board reject the Petition.

Respectfully submitted,

Dated: <u>January 15, 2025</u> Mailing address for all correspondence: Saul Ewing LLP Centre Square West 1500 Market Street, 38th Floor Philadelphia, PA 19102-2186	<u>/Joseph M. Kuo/</u> Brian R. Michalek (Reg. No. 65,816) Saul Ewing LLP 161 North Clark Street, Suite 4200 Chicago, IL 60601 Tel: (312) 876-7151 brian.michalek@saulewing.com Joseph M. Kuo (Reg. No. 38,943) Saul Ewing LLP 161 North Clark Street, Suite 4200 Chicago, IL 60601 Tel: (312) 876-7151 joseph.kuo@saulewing.com Brian Landry (Reg. No. 62,074) Saul Ewing LLP 131 Dartmouth Street, Suite 501 Boston, MA 02116 Tel: (617) 912-0969 Brian.Landry@saulewing.com Andrew Schwerin (Reg. No. 72,999) Saul Ewing LLP 1500 Market Street, 38th Floor Philadelphia, PA 19102-2186 Tel: (215) 972-7184 Andrew.Schwerin@saulewing.com Counsel for Patent Owner
--	---

Certification of Word Count Under 37 C.F.R. § 42.6(d)

The undersigned hereby certifies that the foregoing complies with the type-volume limitation in 37 C.F.R. § 42.24(b)(1). According to the word-processing system's word count, the document contains 13,990 words, excluding the parts of the brief exempted by 37 C.F.R § 42.24(b).

Date: **January 15, 2025**

/Brian R. Landry/
Reg. No. 62,074

Certification of Service Under 37 C.F.R. § 42.6(e)(4)

The undersigned hereby certifies that the foregoing was served in its entirety by filing through the Patent Trial and Appeal Board P-TACTS, as well as providing a courtesy copy via e-mail to the attorneys of record.

Date: **January 15, 2025**

/Brian R. Landry/
Reg. No. 62,074